TREND MICRO | research

VERSO UN NUOVO SLANCIO

LE PREVISIONI SULLA SICUREZZA DI TREND MICRO PER IL 2022

TREND MICRO RESEARCH

VERSO UN NUOVO SLANCIO

LE PREVISIONI SULLA SICUREZZA DI TREND MICRO PER IL 2022

05
Minacce cloud
Le aziende dovranno assicurarsi di adottare i requisiti fondamentali della sicurezza cloud per difendersi da un'ondata di minacce dirette contro questi ambienti e raggiungere un livello di rischio gestito

08
Minacce ransomware
Per rimanere protette dalle minacce ransomware in costante evoluzione, le aziende dovranno difendere i propri server con policy rigide per il controllo di server e applicazioni

11
Sfruttamento delle vulnerabilità
I team della sicurezza dovranno essere ben equipaggiati per contrastare i cybercriminali che riutilizzano le vecchie vulnerabilità e sfruttano quelle appena scoperte, nell'arco di qualche giorno o addirittura di ore

14
Attacchi con malware commodity
I criminali continueranno a considerare le piccole aziende come una facile preda ma le PMI che ricorrono al cloud saranno preparate con misure di sicurezza in grado di neutralizzare gli attacchi commodity

17
Minacce IoT
Le aziende cercheranno di migliorare il monitoraggio e la visibilità di rete per salvaguardare i propri ambienti IT contro le minacce derivanti dalla diffusione dell'IoT

20
Minacce alla supply chain
Nell'irrobustire le proprie supply chain con la diversificazione e la regionalizzazione, le aziende implementeranno principi zero trust, per rendere più sicuri gli ambienti

23
Avanti tutta verso la cybersecurity

A cura di Trend Micro Research

VERSO UN NUOVO SLANCIO

LE PREVISIONI SULLA SICUREZZA DI TREND MICRO PER IL 2022

Il 2021 ha segnato un punto di svolta per le aziende di qualsiasi dimensione, poiché i lockdown hanno spinto molte di esse a velocizzare la propria trasformazione digitale e ad adottare modelli di lavoro ibridi. Oggi, dopo quasi due anni di pandemia, queste stesse aziende devono prepararsi a un altro cambio di marcia mentre il mondo si sta riposizionando nell'ennesima nuova normalità che assegna la priorità al modello di lavoro ibrido e che, si spera, si colloca al termine della crisi sanitaria globale.

I criminali si preparano a sfruttare le opportunità che nascono da uno scenario di business ancora fluido. Nuove criticità sono destinate a emergere mentre la spinta verso la trasformazione digitale continua a ridefinire le superfici di attacco delle aziende, che, tuttavia, dovranno essere pronte a neutralizzare le minacce rafforzando le proprie difese attraverso strumenti e best practice.

Nel 2022 le minacce emergenti continueranno a mettere alla prova la resilienza delle supply chain in tutto il mondo. Il modello di quadrupla estorsione, che ha guadagnato popolarità tra i malviventi, provocherà interruzioni nell'operatività le cui conseguenze non saranno sentite solo dalle vittime dirette ma anche dai loro clienti e partner.

Chi utilizza il cloud dovrà organizzare le proprie difese su molteplici fronti, in particolare se vorrà resistere ad attacchi lanciati da avversari che non ricorrono solo a metodologie ben collaudate ma che innovano anche seguendo le tendenze tecnologiche più recenti. L'introduzione di nuove criptovalute nel 2022 richiederà ai team incaricati della sicurezza di neutralizzare i cybercriminali intenzionati a infiltrarsi nelle risorse aziendali per sfruttarne le capacità di cloud computing. Ci aspettiamo anche che gli aggressori rivolgano sempre più le loro attenzioni verso gli ambienti di sviluppo e le credenziali degli sviluppatori, per stabilire punti di accesso utili a penetrare nei servizi e nelle applicazioni cloud. Di conseguenza, gli sviluppatori dovranno assicurarsi che le proprie credenziali restino fuori dalla portata degli aggressori interessati a comprometterne i sistemi.

Prevediamo che nel corso dell'anno verrà scoperta una quantità di vulnerabilità senza precedenti, conseguenza di un maggior numero di esperti decisi a incassare le relative ricompense e di una accresciuta attenzione dei media nei confronti delle vulnerabilità stesse. Ci aspettiamo che questo conduca a un'esplosione dei cosiddetti exploit zero-day tale da superare il record di quelli utilizzati attivamente nel corso del 2021.[2] Le finestre temporali richieste dalle patch lasceranno le aziende che non si proteggono alla mercé dei malintenzionati decisi a sfruttare qualsiasi punto debole sia presente in un'infrastruttura IT, combinando molteplici vulnerabilità per dare vita a nuove minacce multipiattaforma.

Nell'ecosistema del ransomware vediamo due tendenze nel 2022. Le aziende dovranno rafforzarsi per proteggersi dalle moderne minacce ransomware, che sono destinate a farsi ancora più mirate ed evidenti. I malviventi ricorreranno a metodi estorsivi sempre più complessi, come l'esfiltrazione dei dati e la relativa trasformazione in arma. I loro attacchi costituiranno una sfida per i team responsabili della sicurezza, dato che molte aziende devono ancora investire nella protezione dei server tanto quanto hanno investito sinora nella protezione degli endpoint.

Mentre le grandi aziende saranno impegnate a neutralizzare gli attacchi mirati contro di esse, i criminali equipaggiati con arsenali digitali aggiornati avranno maggior successo nei confronti di realtà più piccole, grazie soprattutto ai broker specializzati in malware che vendono tool "pronti all'uso" tali da rendere gli attacchi una commodity come tante altre. La nuova ondata di malware di questo tipo, che arriverà durante l'anno, probabilmente segnerà l'arrivo di un insidioso modello botnet-as-a-service in grado di compromettere molteplici piattaforme.

Ulteriori sviluppi nel campo dei dispositivi smart stimoleranno l'interesse dell'underground criminale nei confronti degli ambienti IoT (Internet of Things), per andare oltre i dispositivi smart in sé. Infatti, i cybercriminali rivolgeranno l'attenzione verso il volume crescente di dati prodotti dalle vetture connesse, una commodity molto ricercata che promette di aprire nuovi flussi di ricavi per le case automobilistiche. Sarà un'opportunità per spingere i vendor di sicurezza e i produttori di automobili a collaborare, per tracciare la roadmap di una nuova classe di vetture smart sicure.

Il 2022 segnerà il termine di un periodo di transizione ricco di possibilità tanto per le aziende quanto per i cybercriminali. Il presente report approfondisce gli insight e le previsioni dei nostri esperti per l'anno in corso, con l'obiettivo di aiutare le aziende a prendere decisioni maggiormente informate sui vari fronti della sicurezza.

Minacce cloud

Le aziende dovranno assicurarsi di adottare le basi della sicurezza cloud per difendersi da un'ondata di minacce dirette contro questo ambiente e raggiungere così un livello di rischio gestito

I cybercriminali saranno contemporaneamente innovatori e tradizionalisti, adottando un approccio "shift left" per seguire le ultime tendenze tecnologiche e continuando a usare tecniche più che collaudate per colpire gli utenti cloud

Il cloud,[3] con la sua capacità apparentemente infinita di conservare ed elaborare enormi quantità di dati, ha permesso alle aziende di passare al telelavoro con relativa facilità a fronte della pandemia di Covid-19.[4] Anche quest'anno la migrazione verso il cloud resterà un aspetto chiave della nuova normalità operativa delle aziende. Gartner prevede che nel 2022 la spesa globale destinata ai servizi cloud supererà i 482 miliardi di dollari, un aumento del 54% rispetto ai 313 miliardi del 2020.[5] E se è vero che gli utenti saranno impegnati a migrare verso il cloud, i malviventi faranno lo stesso.

Per massimizzare i propri guadagni, i cybercriminali faranno in modo di non tralasciare alcuna possibilità: continueranno a sfruttare tipologie di attacco tradizionali e ben collaudate ma allo stesso tempo faranno leva sulle nuove tendenze tecnologiche per cercare di essere sempre un passo avanti.

Non solo le aziende continueranno a usare applicazioni e soluzioni SaaS (Software-as-a-Service) ma l'adozione di questo modello è destinata ad aumentare ancora nell'anno. Gartner prevede che gli utenti SaaS spenderanno nel 2022 circa 172 miliardi di dollari, l'importo più alto tra tutti i servizi su cloud pubblico.[6] E poiché le tattiche, le tecniche e le procedure (TTP) usate dai malviventi continuano a funzionare – e probabilmente continueranno a funzionare anche contro i nuovi utenti SaaS – la loro diffusione proseguirà anche nel 2022.

I cybercriminali ricorreranno ancora a strategie a basso costo ma ad alto impatto per ottenere accessi alle applicazioni e ai servizi cloud. L'uso di e-mail di phishing per sottrarre credenziali è un esempio di un metodo che resterà diffuso anche quest'anno. Applicazioni e servizi SaaS continueranno a essere compromessi attraverso segreti non protetti,[7] mancanza di rotazione delle chiavi di accesso, immagini container non protette ottenute da fonti inaffidabili[8] e policy di gestione delle identità per il controllo degli accessi immature o implementate in modo carente. In genere, i cybercriminali sono attratti da strategie che funzionano: per questo continuano, per esempio, ad avvalersi di vulnerabilità ormai note, scoperte anni fa, perché molti ambienti sono ancora privi di patch. Oltre a sfruttare le nuove vulnerabilità che saranno scoperte nel corso del nuovo anno, non mancheranno di utilizzare quelle vecchie che ancora funzionano.

Per il 2022 prevediamo che gruppi criminali come TeamTNT continueranno a sfruttare la potenza di calcolo degli ambienti cloud per il mining illecito di criptovalute.[9] Con l'emergere di nuove monete digitali, le unità cybercriminali non smetteranno di approfittarsi delle risorse di cloud computing delle loro vittime attraverso nuove iterazioni di attacchi già visti in passato.

D'altra parte, anche i cybercriminali non mancano di seguire le tendenze tecnologiche. Qualsiasi tecnologia che abbia larga diffusione diventa un obiettivo attraente, come accaduto in passato per tecnologie come Java,[10] Adobe Flash,[11] e WebLogic.[12]

Una conseguenza interessante, anche se negativa, della tecnica "shift left" è che i cybercriminali inizieranno a utilizzare nei propri attacchi sempre più spesso questo approccio. Stiamo già verificando attività di malintenzionati rivolte contro tool e pipeline DevOps[13] all'interno di ambienti IDE (Integrated Development Environment) in cloud.[14] Prevediamo che i cybercriminali creeranno ulteriori campagne utilizzando principi DevOps contro supply chain, ambienti Kubernetes, implementazioni IoC (Infrastructure-as-Code) e pipeline. Ci aspettiamo, inoltre, che gli sviluppatori e i sistemi usati per le build saranno sfruttati come punti di ingresso da parte degli attaccanti intenzionati a diffondere malware all'interno di più aziende attraverso attacchi supply chain. I token e le password degli sviluppatori contengono le chiavi delle operazioni delle aziende e riuscire a usare le credenziali compromesse di uno sviluppatore aumenta le possibilità di far passare inosservato il rilascio del malware.

L'adozione del cloud è un elemento fondamentale della trasformazione digitale. È quindi importante che le aziende proteggano in modo adeguato gli ambienti cloud secondo le basi essenziali della sicurezza del cloud, come la comprensione e l'applicazione del modello di responsabilità condivisa,[15] l'uso di un framework ben architettato,[16] l'impiego della crittografia, la regolare applicazione delle patch[17] e l'acquisizione del giusto livello di competenze. Le aziende devono anche far osservare protocolli di sicurezza più stringenti relativamente ai sistemi per le build e al codice scritto dagli sviluppatori, in particolare se il codice influisce su processi di produzione importanti. A questo scopo i team incaricati della sicurezza possono applicare misure come la gestione dei privilegi con token d'accesso a durata limitata, sviluppare tracce di audit per mezzo di tool a linea di comando e monitorare la pipeline attraverso software open source per la gestione della sicurezza.

Minacce ransomware

Per restare al sicuro da minacce ransomware in costante evoluzione, le aziende dovranno proteggere i propri server con stringenti policy per il controllo di server e applicazioni

I server saranno il principale obiettivo dei ransomware

Come qualsiasi minaccia digitale, anche il ransomware[18] evolve con regolarità. In passato gli incidenti legati al ransomware usavano di solito gli endpoint come punti di accesso iniziali: le vittime cadevano nel tranello aprendo messaggi e-mail appositamente preparati o visitando siti web che installavano furtivamente un payload contenente il ransomware.[19] Ma con l'avvento della pandemia abbiamo registrato un cambiamento evidente nel modo di condurre questo genere di attacchi.

Gli attaccanti, per accedere ai loro bersagli aziendali, si stanno ora concentrando su servizi esposti e su compromissioni server-side. E con il lavoro ibrido, un modello in cui i dipendenti lavorano sia da remoto sia on-site e che rappresenta la nuova normalità per le aziende,[20] prevediamo che questa tendenza continuerà anche nel nuovo anno. Il modello del lavoro ibrido ha molti pro, come maggiori livelli di flessibilità e produttività, ma presenta anche aspetti indiscutibilmente negativi sul fronte della cybersecurity. A causa della più ampia superficie di attacco offerta da server e ambienti di lavoro domestici poco sicuri, è difficile capire come gli attaccanti entrano e agiscono e come i team incaricati della cybersecurity possano bloccare immediatamente gli attacchi ransomware.

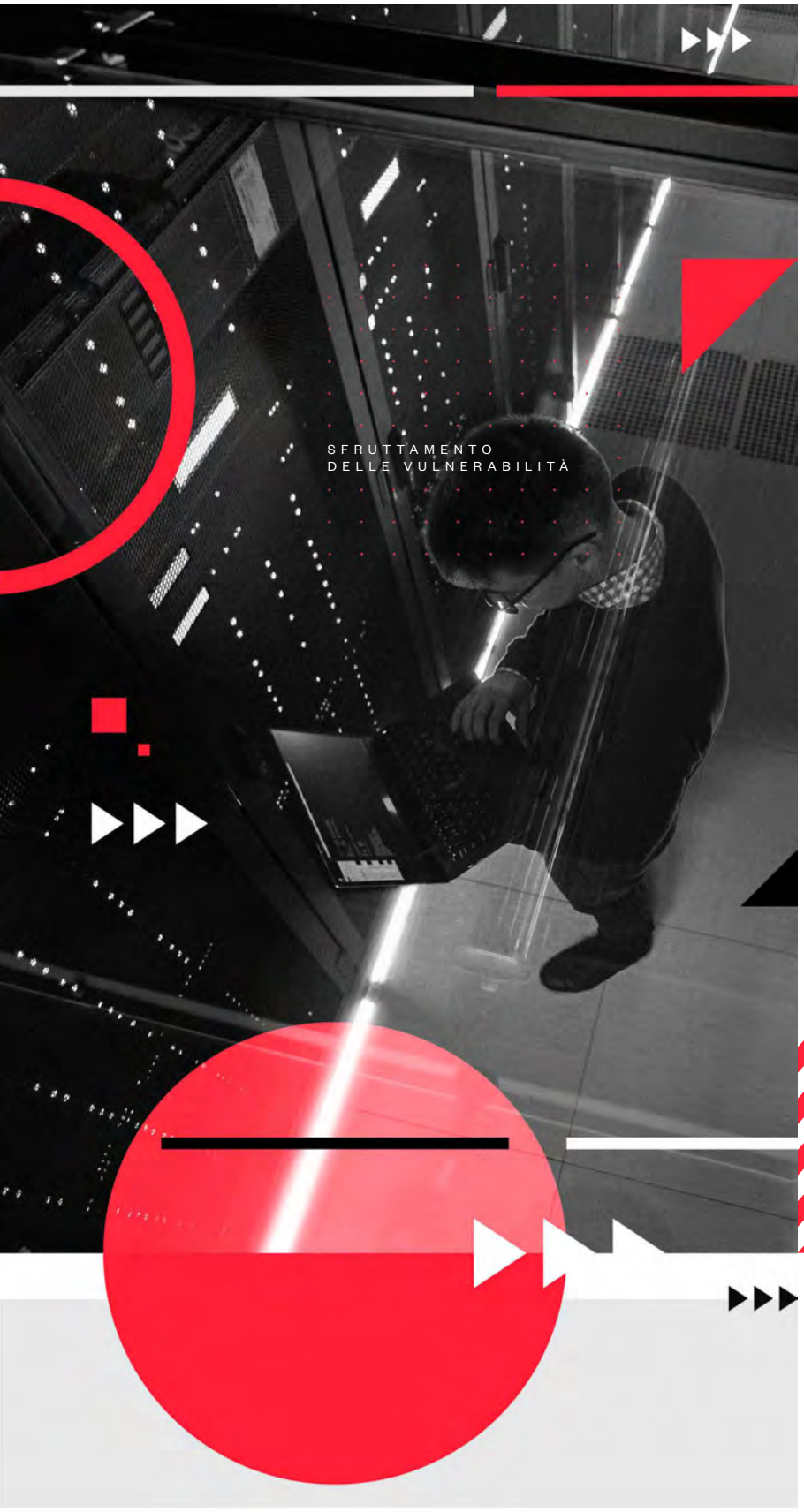
In base agli incidenti che abbiamo osservato l'anno scorso ci aspettiamo anche di assistere a due importanti sviluppi nell'evoluzione del ransomware durante il 2022.[21] Primo, gli attacchi ransomware diventeranno ancora più mirati e penetranti, rendendo più difficile la difesa di reti e sistemi da parte delle aziende. Poiché il ransomware moderno è relativamente nuovo, è assolutamente possibile che le aziende debbano ancora investire nella difesa e nella mitigazione di queste minacce nell'ambito dei server allo stesso modo in cui finora hanno agito nell'ambito degli endpoint. Esiste, inoltre, la continua carenza di esperti specializzati in cybersecurity che è un'aggravante nella protezione delle aziende contro le minacce ransomware.[22] Le TTP utilizzate dagli attaccanti resteranno probabilmente le stesse ma saranno dirette contro obiettivi più complessi, possibilmente più grandi rispetto a quelli colpiti negli anni passati.

Il secondo sviluppo che prevediamo riguarda il ricorso da parte dei criminali a metodi di estorsione più sofisticati e moderni simili agli APT (Advanced Persistent Threat) utilizzati negli attacchi sferrati da entità paragovernative.[23] Una volta riusciti a infiltrarsi negli ambienti delle loro vittime, gli attaccanti possono scegliere se limitarsi a esfiltrare i dati sensibili e ricattare le loro vittime evitando tutto il passaggio che comporta la cifratura crittografica o il blocco degli accessi. In termini di successo delle campagne di estorsione, l'attenzione si sposterà dall'impedire l'accesso ai dati critici per passare invece all'estrazione e diffusione dei dati. I vettori di attacco usati per colpire le aziende con il ransomware, come VPN (Virtual Private Network), e-mail di spear-phishing e porte RDP (Remote Desktop Protocol) esposte, resteranno in voga. Tuttavia, nel 2022 il cloud sarà colpito con più frequenza. Sempre più aziende migrano infatti verso il cloud[24] portando con sé il proprio patrimonio di dati e risorse sensibili e questo spinge i cybercriminali a seguirne i passi.[25]

Oltre a implementare best practice di sicurezza per proteggere i server, le aziende potranno trarre vantaggio da un rigido rispetto delle guideline di rafforzamento dei server per tutte le applicazioni e i sistemi operativi pertinenti. Garantire la corretta configurazione dei server aiuta le aziende a difendersi dai ransomware e da altre minacce.

Poiché i server possiedono una gamma prevedibile di applicazioni basata sui loro ruoli specifici, è anche consigliabile adottare tecniche di controllo delle applicazioni, una pratica che permette di bloccare o limitare le applicazioni tranne quelle che vengono esplicitamente autorizzate dai team IT.

Sfruttamento delle vulnerabilità



I team incaricati della sicurezza dovranno essere ben equipaggiati per contrastare criminali che riutilizzano le vecchie vulnerabilità e sfruttano quelle appena scoperte nell'arco di qualche giorno o addirittura di ore

Le aziende nel 2021 hanno dovuto far fronte a un numero record di vulnerabilità zero-day e sono diventate più accorte. Per questo resteranno vigili rispetto alle eventuali finestre che possono aprirsi nelle procedure di patching, poiché verranno sicuramente identificate ulteriori vulnerabilità

Il 2022 promette di rivaleggiare in quanto a record assoluto di vulnerabilità zero-day che hanno contribuito a definire lo scenario delle minacce cyber nel 2021: sono 66 quelle rilevate in-the-wild al momento della redazione del presente report, il numero più alto da quando si tiene traccia di questo parametro.[26] Prevediamo che nel 2022 verranno scoperte in-the-wild ancora più vulnerabilità zero-day, il che non significa necessariamente una flessione nella qualità del codice bensì indica il contributo di varie concause come un crescente interesse da parte dei media nell'occuparsi di exploit da prima pagina, cacciatori di vulnerabilità attirati da ricche ricompense[27] come quelle offerte dalla Zero Day Initiative (ZDI) di Trend Micro allo scopo di prevenire gli attacchi zero-day,[28] ed errori di implementazione destinati a emergere mentre sempre più aziende effettuano la propria trasformazione digitale. È possibile che gli operatori della cybersecurity identifichino solo una porzione delle vulnerabilità attivamente sfruttate, pertanto la scoperta di un maggior numero di esse è anche l'indicatore di un aumento dell'efficacia dei metodi di rilevamento e di un cambio di atteggiamento nei confronti della disclosure.[29] I programmi di bug bounty hanno compiuto grandi passi avanti in direzione di un rilevamento anticipato delle vulnerabilità a vantaggio delle aziende, come dimostrato dal modo in cui gli incentivi di ZDI hanno contribuito allo sviluppo di patch virtuali per i clienti della soluzione di sicurezza Trend Micro™ TippingPoint™, con una media di 81 giorni di anticipo rispetto alle patch pubblicamente rilasciate dai rispettivi vendor nel 2019.[30]

Tuttavia, se il successo delle passate edizioni del concorso di hacking Pwn2Own[31] è di qualche indicazione, la finestra di opportunità per sfruttare una vulnerabilità sarà ridotta a pochi giorni, se non addirittura poche ore, e saranno disponibili exploit per vulnerabilità risolte nelle versioni beta prima che le patch di sicurezza siano rilasciate nel prodotto finale. Il cosiddetto "patch gap" – ovvero il tempo che intercorre tra la scoperta di una vulnerabilità e il rilascio della patch che la neutralizza – resterà una miniera d'oro per gli attaccanti che senza dubbio faranno affidamento sui ritardi nel rollout dei bug fix critici per guadagnare il tempo necessario a sviluppare i loro exploit. Ritardi nel deployment programmato delle patch possono avvenire quando i bug fix devono superare i collaudi software, come quando l'engine JavaScript V8 di Google Chrome è stato reso disponibile agli utenti di questo browser con la versione 77 di Chrome nel settembre 2019, un mese dopo che il bug di V8 era stato già corretto.[32] Ciò lascia le aziende in posizione scomoda, dal momento che devono affrontare la duplice difficoltà di prevedere un'accelerazione degli exploit nel periodo di attesa dei bug fix e implementare questi ultimi non appena vengono rilasciati. Affrontare queste vulnerabilità non è un processo uniforme; per esempio, applicare patch agli endpoint è un lavoro molto più lineare rispetto a quanto accade sui server, per i quali si incorre spesso in costi maggiori dovuti alle interruzioni operative necessarie.[33]

Invece di studiare attivamente intere porzioni di codice alla ricerca di errori, i cybercriminali inizieranno a usare le patch come comodi indicatori di problemi all'interno di un sistema e personalizzare poi il codice del proprio malware. Nel 2022 ci sarà un segmento di cybercriminali dedicato a monitorare le aziende in vista di qualunque vulnerabilità annunciata e patch implementata, così da velocizzare i propri attacchi.

I cybercriminali non stanno solo pianificando di sfruttare le nuove vulnerabilità ma continueranno anche a capitalizzare quelle vecchie. Ciò non farà che sottolineare ulteriormente la necessità di dare priorità alla gestione delle patch da parte delle aziende e dei vendor loro partner. Le vulnerabilità scoperte negli scorsi anni resteranno rilevanti, dato che verranno riutilizzate e combinate insieme per potenziare gli attacchi che saranno sferrati nel nuovo anno. Allo stesso modo ci sarà un'ondata di attacchi misti diretti contro più prodotti software a cascata, per esempio collegando a catena le vulnerabilità di Google Chrome con quelle di Microsoft Windows per ottenere accesso privilegiato ai sistemi. Una conseguenza positiva di questa tecnica è che attirerà inevitabilmente l'attenzione degli analisti verso superfici di attacco finora poco considerate. Ci aspettiamo un aumento del lavoro di ricerca sulle tecnologie server-side che possa evidenziare i punti deboli di piattaforme come Microsoft Exchange e SharePoint così da mitigare l'impatto di qualsiasi attacco futuro sui loro utenti finali.

Anche la sicurezza cloud-native dovrà essere una priorità per le aziende, molte delle quali hanno adottato il cloud dopo che la pandemia ne ha accelerato la trasformazione digitale. La dipendenza di molti progetti cloud-native da librerie basate su software open source potrebbe lasciarli esposti ad attacchi che combinano vulnerabilità note, dal momento che queste librerie spesso non vengono mantenute aggiornate né verificate sistematicamente rispetto a errori noti.[34] Per i team incaricati della sicurezza, riuscire a trovare fonti affidabili per tenere traccia delle vulnerabilità cloud sarà essenziale al fine di proteggere le risorse cloud, poiché continua a esserci carenza di report CVE (Common Vulnerabilities and Exposures) relativi a bug on-premises correlati al cloud.[35]

Ora più che mai, le aziende dovranno assicurarsi che i loro team dedicati alla sicurezza IT siano pronti per adattarsi ad affrontare quest'imminente ondata di exploit. Ciò significa fornire a questi team il supporto e le risorse che occorrono per inventariare i dispositivi presenti nell'ambiente IT attraverso soluzioni di asset management, monitorare gli aggiornamenti di sicurezza dei vendor per reagire non appena le vulnerabilità vengono annunciate pubblicamente e implementare il patching virtuale[36] o l'isolamento delle macchine per proteggere qualsiasi punto d'ingresso da potenziali minacce.

Attacchi con malware commodity

I criminali continueranno a considerare le piccole aziende come una facile preda ma le PMI che ricorrono al cloud saranno preparate con misure di sicurezza in grado di neutralizzare gli attacchi commodity

Mentre tutta l'attenzione è rivolta al ransomware, i tradizionali attacchi commodity e as-a-service avranno tempo di innovare tool molto più sofisticati

Le grandi imprese rimarranno una ricca preda per i criminali intenzionati a lucrare forti riscatti mediante ransomware ma gli exploit da prima pagina dei gruppi più abili lasceranno le PMI esposte agli attacchi degli affiliati a servizi RaaS (Ransomware-as-a-Service) e dei piccoli cybercriminali che sfruttano malware commodity e mantengono un basso profilo.[37]

Negli ultimi anni l'attenzione del pubblico si è concentrata sul ransomware, che è considerato un tipo di malware commodity e un modello as-a-service. Ma nei circoli cybercriminali sono diffuse anche altre tipologie di malware pacchettizzato come RAT (Remote Access Trojan), stealer per la sottrazione di informazioni, miner di criptovalute, dropper e malware loader. Tutto questo farà crescere il mercato dei malware commodity fino a diventare una minaccia insidiosa e tremenda. Gli operatori di ransomware hanno messo a frutto i tool dei malware commodity per rendere più efficaci i loro attacchi[38] mentre altri malintenzionati hanno usato gli stessi strumenti per lanciare campagne motivate politicamente.[39] Nel caso del ransomware è stato osservato l'impiego di tool come Cobalt Strike, Koadic, PowerShell Empire e Metasploit[40] in combinazione con le utility di amministrazione legittimamente presenti – una tecnica che fa sopravvivere il malware con le risorse che riesce a reperire nel sistema colpito, quali esse siano – in modo da evitare il rilevamento.[41]

Questi tool vengono forniti con funzionalità avanzate a costi contenuti, rendendo questo genere di malware accessibile ai malintenzionati che intendono arricchire la varietà dei loro arsenali.[42] Molti componenti malware customizzati vengono successivamente pacchettizzati in commodity nell'underground cybercriminale affinché possano essere usati anche da altri criminali[43] Questo porta a prevedere che la prossima generazione di cybercriminali sarà ancora più innovatrice e meglio equipaggiata rispetto a quella che, circa quindici anni fa, ha dato origine allo sviluppo del ransomware.[44] Ci aspettiamo che il mercato dei tool per gli attacchi commodity maturerà e fornirà anche gli strumenti per ampliare le reti di contatti e collaborare con "colleghi" del ramo. Dopo tutto, chi vende malware pronto all'uso non si limita solo a crearli ma è solito arricchire la propria offerta con istruzioni, suggerimenti e guide per la risoluzione degli inconvenienti.[45]

Il modello basato sul servizio, nel quale il malware commodity è venduto nell'ambito di contratti di servizio invece che come prodotto acquistabile una tantum, sarà particolarmente adatto ai malviventi meno preparati, che evolveranno dal fornire semplici tool malware alla ricerca di partner affidabili con cui crescere, per diventare più esperti. Collaborazioni di questo genere porteranno ad attività criminali più resilienti, come evidenziato dal modo in cui i cybercriminali sono stati in grado di ricostruire la botnet di Emotet sfruttando quella di Trickbot, un trojan bancario, solo pochi mesi dopo che l'infrastruttura originale di Emotet era stata smantellata dalle forze dell'ordine.[46]

A causa di questo, prevediamo che nel 2022 gli attacchi commodity raggiungeranno un punto nel quale i criminali inizieranno ad avere minor necessità di sviluppare malware su misura; in tal caso sarà necessario un malware capace di gestire al meglio gli affiliati durante attacchi mirati complessi.

Sulla scorta di queste considerazioni, il settore del malware commodity è più che maturo per un'offerta maggiormente sofisticata con la quale i criminali possano aggiornare i propri armamenti. Quest'anno assisteremo probabilmente al debutto di soluzioni botnet-as-a-service progettate per compromettere e controllare in simultanea piattaforme IoT e piattaforme basate su cloud, proprio come una versione potenziata della botnet ZeuS.[47] È possibile che un tool di questo genere scaturisca dall'underground cybercriminale di lingua russa, noto per le proprie capacità di innovazione,[48] ma anche FreakOut è una botnet che si sta proponendo come valida concorrente continuando a evolvere con funzionalità aggiuntive.[49]

Prevediamo che il mercato degli attacchi commodity, il cui modello di business si affida al codice del malware per fare il grosso del lavoro sostituendosi a un attaccante che si muova all'interno di una rete, si rivelerà largamente inefficace contro le difese più solide comunemente diffuse negli ambienti enterprise, come i sistemi di sicurezza che ricorrono al machine learning.[50] Tuttavia prevediamo anche che nel 2022 i tool malware di questo tipo riscontreranno maggior successo quando usati contro le PMI, venendo adoperati da malviventi che sperano di incontrare difese meno efficaci e meno competizione da parte di altri cybercriminali. In particolare, prevediamo che i dispositivi IoT usati dalle PMI saranno gli obiettivi principali di questi attacchi. Le PMI dovranno essere, quindi, più accorte nella selezione dei vendor acquistando i dispositivi IoT da produttori che storicamente hanno una solida capacità di rilasciare patch su base continuativa.

Solo raramente le PMI possiedono team dedicati alla sicurezza e anche in quel caso tali team sono spesso limitati dalla scarsa disponibilità di fondi dal momento che la cybersecurity è considerata un puro costo operativo. A livello globale la spesa dedicata alla cybersecurity si avvia superare i 150 miliardi di dollari alla fine del 2021[51] ma le PMI investono ogni anno in soluzioni per la sicurezza IT solo più di 40 miliardi restando, quindi, un mercato sotto servito nel quale solo le realtà più mature impiegano esperti interni.[52] A causa di questi budget limitati, prevediamo che molte PMI renderanno prioritaria la protezione degli endpoint, seguita da quella delle loro reti. Alcune PMI saranno tuttavia meglio preparate di altre. Quelle maggiormente basate su ambienti online, che fanno ampio ricorso a servizi e piattaforme cloud-based, proprio per la natura delle loro attività saranno le più consapevoli dei rischi provocati dai malware commodity nei confronti delle operazioni mission-critical. Queste aziende sono quelle che più facilmente metteranno la sicurezza in cima alle loro priorità considerando le soluzioni di cybersecurity come una delle tante voci che formano il costo del venduto.

Minacce IoT

Le aziende cercheranno di migliorare il monitoraggio e la visibilità di rete per salvaguardare gli ambienti IT contro le minacce derivanti dalla diffusione dell'IoT

Le informazioni associate all'IoT diventeranno merce richiesta nell'underground cybercriminale, spingendo le aziende a occuparsi delle lacune nella sicurezza che potrebbero portare alla sottrazione o alla manomissione di dati

I dispositivi smart sono da tempo un obiettivo allettante agli occhi dei criminali che puntano sul fatto che le limitate capacità computazionali presenti nella maggior parte dei dispositivi IoT lasciano ben poco spazio all'integrazione di soluzioni di sicurezza.[53] Dispositivi IoT violati sono stati usati in attacchi di diverso genere compresi quelli di tipo DDoS (Distributed Denial of Service).[54] Poiché sempre più aziende sono state spinte verso la trasformazione digitale per rimanere competitive o almeno operative durante il lockdown, prevediamo un aumento delle minacce cyber rivolte contro di esse, in particolare quelle che si occupano di smart manufacturing, in concomitanza col passaggio verso un modello di lavoro ibrido e il continuo ricorso a servizi di connessione remota.

Per mantenere sicure le proprie attività operative, le aziende il cui personale utilizza dispositivi IoT dovranno adottare nel prossimo anno sistemi IPS/IDS per la prevenzione e il rilevamento delle intrusioni, tool per l'analisi forense delle reti (NFT), tool per il rilevamento delle anomalie nei comportamenti di rete (NBAD) e tool di rilevamento e risposta (NDR) che possano aiutarle a tenere sotto controllo quanto avviene nelle rispettive reti. Chi si avvale del cloud e si affida, quindi, a vendor specializzati in sicurezza dovrà monitorare con attenzione l'utilizzo delle risorse cloud alla ricerca di attività anomale, dovrà salvaguardare i propri ambienti VPC (Virtual Private Cloud) dagli attacchi che potrebbero essere condotti all'interno delle infrastrutture cloud e dovrà verificare le capacità dei potenziali vendor rispetto alle proprie esigenze effettive.

Nel 2022, però, i criminali saranno mossi da aspirazioni ben superiori rispetto all'assumere il controllo di gadget IoT per disporre di una comoda base di attacco per ulteriori attività criminali o potersi spostare lateralmente all'interno di una rete. I cybercriminali si lanceranno presto in una nuova corsa all'oro scatenata dai produttori di automobili – compresi grandi nomi del settore come General Motors, Honda e Toyota[55] – decisi a guadagnare dal traffico dei dati prodotti dalle vetture connesse o veicoli equipaggiati con una serie di telecamere, laser e altri sensori che registrano collettivamente le condizioni di guida e il comportamento del guidatore, comprese le velocità e le distanze percorse da un'auto, e i contenuti di intrattenimento consumati dai passeggeri. Insight in tempo reale di questo genere hanno una miriade di applicazioni per i clienti commerciali, dalla misurazione del successo di una pubblicità al rilevamento della domanda dei consumatori fino al calcolo degli sconti sui premi assicurativi in base ai dati di guida.[56] Questi stessi dati potrebbero essere sfruttati anche dai produttori per monitorare le prestazioni dei vari componenti presenti in un veicolo così da migliorare le rispettive supply chain.[57]

La domanda di informazioni prodotte dalle smart car è destinata a scatenare il boom di un nuovo business con un giro d'affari stimato tra i 450 e i 750 miliardi di dollari entro il 2030[58] senza alcun segno di prevedibile flessione: si calcola che nel 2025 le vetture connesse produrranno10 exabyte di dati al mese.[59] Con la diffusione di questi veicoli sulle strade, i malviventi cercheranno di trasformare l'aumentata connettività in una fonte di illeciti guadagni, tanto che ci aspettiamo un incremento nella richiesta di filtri illegali in grado di bloccare la trasmissione dei dati di rischio o di hacker disponibili a eliminare le tracce di una cattiva condotta di guida dalle registrazioni di una smart car. L'architettura delle smart car potrà essere ulteriormente razionalizzata qualora una porzione più ampia delle sue funzioni e dei suoi processi di raccolta dati di maggior complessità venga spostata nel cloud – tant'è che un numero significativo di applicazioni e sistemi in uso nei modelli di smart car più recenti risiede già su server cloud di back-end[60] – ma questo potrebbe esporre i produttori ad altre minacce come attacchi DoS (Denial-of-Service) e MitM (Man-in-the-Middle).[61]

Se desiderano rendere i loro prodotti a prova di futuro, nel 2022 i produttori di automobili dovranno lavorare a stretto contatto con vendor specializzati per decidere insieme come implementare la sicurezza. Esempi di partnership del genere esistono già. Vi sono già state le prime iniziative come la Open EV Software Platform, promossa dal consorzio Mobility in Harmony (MIH) e dai suoi partner Arm, Microsoft e Trend Micro.[62] È in atto anche una collaborazione tra Volkswagen e Microsoft finalizzata alla creazione di una piattaforma cloud-based utilizzabile per sviluppare soluzioni di guida automatizzata più avanzate e sicure per i veicoli connessi.[63] Progetti di questo tipo getteranno le basi su cui il settore automobilistico potrà sviluppare un sistema operativo dedicato alle vetture smart, con l'obiettivo finale di un ecosistema automotive basato su un sistema operativo unificato che consentirà di dotare i futuri modelli di automobili connesse con funzionalità di sicurezza standardizzate.

Minacce alla supply chain

Nel rinforzare le loro supply chain mediante diversificazione e regionalizzazione, le aziende implementeranno principi zero trust per rendere più sicuri i loro ambienti

Mentre le aziende saranno impegnate a farle evolvere, le supply chain di tutto il mondo saranno nel mirino di tecniche di quadrupla estorsione

La pandemia di Covid-19 ha acceso i riflettori sulla fragilità delle supply chain. Ritardi e scarsità di merce sono le conseguenze di diversi fattori come l'aumento della domanda,[64] l'insufficienza di container e di operatori disponibili[65] e l'adozione di processi di produzione più agili scaturiti dal modello just-in-time.[66] Quando le complicazioni delle supply chain sono diventate un problema per tutto il mondo, anche il valore delle supply chain stesse si è fatto più evidente – non solo per le aziende in difficoltà ma anche per i cybercriminali che nella pandemia hanno trovato nuova benzina per le loro attività. In particolare, quest'anno gli attacchi alle supply chain si sono mischiati sempre più spesso con campagne ransomware, come nel caso degli attacchi REvil/Sodinokib[67] lanciati contro grandi aziende fra cui Quanta Computer,[68] JBS Foods[69] e Kaseya.[70]

Approfittando dei problemi della supply chain e aggravandoli, nel 2022 i cybercriminali aumenteranno il ricorso al modello di quadrupla estorsione.[71] Per sfruttare al massimo i cyberattacchi, costringeranno infatti le loro vittime a pagare ingenti somme di denaro attraverso una tecnica estorsiva che si snoda su quattro direttrici: tenere in ostaggio i dati critici della vittima fino al pagamento di un riscatto, minacciare la diffusione delle informazioni e la pubblicizzazione della violazione, minacciare attacchi ai clienti della vittima e, infine, attaccare la supply chain dei fornitori.

Nel 2021 il gruppo cybercriminale DarkSide ha attaccato Colonial Pipeline, il più vasto sistema di distribuzione di greggio raffinato degli Stati Uniti. Il gruppo ha impedito all'azienda di accedere ai suoi sistemi informativi e ha sottratto oltre 100 GB di dati corporate.[72] È stato osservato come questo gruppo abbia regolarmente innovato le proprie strategie di attacco offrendo anche servizi DDoS e di call center.[73] In questo modo gli affiliati a DarkSide possono lanciare attacchi a quadrupla estorsione che possono avere pesanti conseguenze sulle supply chain. Di conseguenza, i malviventi potrebbero impedire l'accesso a dati critici come segreti industriali, bloccare macchinari usati in produzione o contattare clienti e stakeholder per far pressione sulle vittime spingendole a pagare.

Le supply chain saranno oggetto, inoltre, di attenzione da parte dei broker AaaS (Access-as-a-Service). Una volta che ambienti vulnerabili siano stati compromessi con successo, i broker AaaS possono vendere ad altri cybercriminali l'accesso alle reti aziendali, gli account amministrativi e le credenziali di autenticazione a fronte di somme variabili.

I cambiamenti economici generati dalla pandemia spingeranno le aziende a investire nei processi di sviluppo delle proprie supply chain e a concentrarsi sul rendere più solide le relative operazioni per mezzo della diversificazione. Per anni i vari Paesi hanno percorso la via della globalizzazione, criticata come causa di un eccessivo affidamento nei confronti di un'unica fonte geografica per tutti gli approvvigionamenti.[74] Al posto della globalizzazione, le operazioni di supply chain passeranno ora alla regionalizzazione, assicurando in questo modo che le aziende rispondano agli aumenti della domanda e alla volatilità dei costi di produzione. Le strategie di diversificazione cambieranno da un'azienda all'altra: alcuni anelli delle catene di fornitura resteranno locali mentre altri verranno dislocati in Paesi o regioni differenti.

Tuttavia, la diversificazione non è un traguardo facilmente raggiungibile in modo appropriato e sicuro e può essere uno sforzo decisamente impegnativo in termini di costi e di risorse. Le aziende che si rivolgono a fornitori più vicini a casa propria per ridurre i rischi economici e aiutare a sostenere le attività di business potrebbero anche inconsapevolmente aprire le porte a rischi di sicurezza. Fornitori tradizionali con cui si è lavorato per anni saranno rimpiazzati da nuove aziende che andranno comunque valutate e verificate. Questi nuovi fornitori potrebbero offrire servizi e applicazioni cloud con policy di sicurezza insoddisfacenti o magari non dare del tutto importanza alla sicurezza cloud.

Il periodo nel quale due organizzazioni allineano i rispettivi processi è critico e i malviventi possono sferrare attacchi mirati per sfruttare i cambiamenti e la scarsa familiarità associata alle partnership di nuova costituzione. Per esempio, un criminale potrebbe spacciarsi per il dipendente di un nuovo fornitore e inviare una mail di spear-phishing richiedendo al destinatario di compilare un modulo informativo su un sito web fasullo.

Per mantenere protette le supply chain mentre le aziende fanno evolvere le loro strategie, bisognerebbe applicare l'approccio zero trust in tutte le procedure legate alla sicurezza.[75] Il modello zero trust aiuta a salvaguardare le modalità attraverso cui le aziende interagiscono e si scambiano dati con continue verifiche per tutto il periodo di una connessione. Grazie a questo modello le aziende possono essere certe che lo stato di salute di utenti, dispositivi, applicazioni e servizi con cui interagiscono resti costantemente monitorato e valutato.

Avanti tutta verso la cybersecurity

Le nostre previsioni sullo scenario della sicurezza per il 2022 tratteggiano le minacce e i rischi che emergono dalle ricerche, dalle osservazioni e dagli insight dei nostri esperti sulle tecnologie del settore e sulle preoccupazioni in circolazione. Nell'affrontare queste problematiche, le aziende potranno trarre vantaggio da una strategia di cybersecurity olistica e multistrato che tenga conto delle seguenti raccomandazioni:

Tornare alle basi essenziali della sicurezza. Potrà sembrare semplice ma rispettare le best practice di sicurezza può aiutare le aziende a contrastare la maggior parte delle minacce vecchie e nuove anche nel 2022. I malviventi continueranno a sfruttare le vulnerabilità di sistemi e applicazioni già note; pertanto, è essenziale che le aziende dispongano di policy appropriate per la gestione delle patch. Ciò aiuterà a evitare le violazioni dei dati e, di conseguenza, i costi delle relative sanzioni e i danni alla reputazione. Le aziende dovrebbero inoltre comprendere e applicare il modello di responsabilità condivisa e cifrare regolarmente i dati critici.

Applicare il modello zero trust per tenere al sicuro ambienti e applicazioni. Le aziende possono rafforzare la security posture adottando il modello zero trust, un approccio nel quale ogni utente o dispositivo che tenti di connettersi ad applicazioni o sistemi deve essere verificato sia prima di ottenere l'accesso sia regolarmente anche in seguito, indipendentemente dal fatto che si trovi all'interno della rete o meno.

Rafforzare la sicurezza dei server e adottare il controllo degli accessi. Spostandosi verso un modello di lavoro ibrido, è essenziale per le aziende definire e implementare policy di sicurezza che tengano conto assenza di perimetri tipica dell'ambiente di lavoro emerso in seguito alla pandemia. Il controllo di applicazioni e accessi può consentire alle aziende di gestire meglio la propria sicurezza generale anche quando i dipendenti accedono a dati e applicazioni sensibili dall'esterno e con dispositivi differenti.

Dare priorità alla visibilità. Anche nel nuovo anno i dipendenti continueranno ad accedere da remoto ad applicazioni, servizi, sistemi e database in cloud. Per questo è importante ottenere ampia visibilità così da contribuire a rafforzare le difese della cybersecurity. I team incaricati della sicurezza devono essere consapevoli di tutti i provider, account e servizi cloud esistenti in modo da tenerli monitorati e accertarsi che siano configurati nel modo più sicuro possibile. Ciò contribuirà a minimizzare il rischio di configurazioni errate ed esposizioni involontarie.

Passare a una sicurezza più solida con le giuste soluzioni e il giusto livello di competenze. Per proteggere i propri ambienti e sistemi da minacce in costante evoluzione, le aziende hanno bisogno di soluzioni flessibili, automatizzate e avanzate capaci di rilevare con efficienza gli attacchi sferrati tramite e-mail e contro endpoint, reti, server e workload in cloud. Trend Micro fornisce dettagli analitici completi e insight di sicurezza redatti da un team di analisti dedicati che hanno accesso a enormi volumi di analytics, potenti soluzioni per la sicurezza e di intelligence globale sulle minacce.

Bibliografia

1. Julie Steenhuysen. (Nov. 3, 2021). *Reuters.* "Analysis: Country by country, scientists eye beginning of an end to the COVID-19 pandemic." Accessed on Nov. 25, 2021, at https://www.reuters.com/business/healthcare-pharmaceuticals/country-by-country-scientists-eye-beginning-an-end-covid-19-pandemic-2021-11-03/.
2. Joe Devanesan. (Oct. 20, 2021). *TechHQ.* "2021 was a record-breaking year in zero-day exploits – that's both good and bad news." Accessed on Nov. 19, 2021, at https://techhq.com/2021/10/2021-was-a-record-breaking-year-in-zero-day-exploits-and-thats-both-good-and-bad-news/.
3. Trend Micro. (Oct. 24, 2019). *Trend Micro Security News.* "The Cloud: What it is and what it's for." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/vinfo/us/security/news/security-technology/the-cloud-what-it-is-and-what-it-s-for.
4. Trend Micro. (Oct. 7, 2020). *Trend Micro Security News.* "CSO Insights: DataBank's Mark Houpt on Looking Beyond Securing Infrastructures in the New Normal." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/vinfo/us/security/news/security-technology/cso-insights-databank-mark-houpt-on-looking-beyond-securing-infrastructures-in-the-new-normal/.
5. Bernard Marr. (Oct. 25, 2021). *Forbes.* "The 5 Biggest Cloud Computing Trends In 2022." Accessed on Nov. 10, 2021, at https://www.forbes.com/sites/bernardmarr/2021/10/25/the-5-biggest-cloud-computing-trends-in-2022/.
6. Gartner. (Aug. 2, 2021). *Gartner.* "Gartner Says Four Trends Are Shaping the Future of Public Cloud." Accessed on Nov. 10, 2021, at https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud.
7. David Fiser and Alfredo Oliveira. (June 29, 2021). *Trend Micro Research, News, and Perspectives.* "Secure Secrets: Managing Authentication Credentials." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/research/21/f/secure_secrets_managing_authentication_credentials.html.
8. Chuck Losh. (May 18, 2021). *Trend Micro Research, News, and Perspectives.* "Container Security First Steps: Image and Registry Scanning." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/devops/21/e/container-security-first-steps-image-and-registry-scanning.html.
9. Trend Micro. (July 20, 2021). *Trend Micro Security News.* "TeamTNT Activities Probed: Credential Theft, Cryptocurrency Mining, and More." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/teamtnt-activities-probed.
10. Trend Micro. (Sept. 10, 2013). *Trend Micro Research, News, and Perspectives.* "How the Java Security Situation Quietly Got Much Worse." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/research/13/i/java-security-situation-quietly-got-much-worse.html.
11. Trend Micro. (Feb. 2, 2015). *Trend Micro Research, News, and Perspectives.* "New Adobe Flash 0-Day Exploit Used in Malvertisements." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/research/15/b/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements.html.
12. Catalin Cimpanu. (May 1, 2020). *ZDNet.* "Oracle warns of attacks against recently patched WebLogic security bug." Accessed on Nov. 10, 2021, at https://www.zdnet.com/article/oracle-warns-of-attacks-against-recently-patched-weblogic-security-bug/.
13. Trend Micro. (n.d.). *Trend Micro Security News.* "DevOps Definition Page." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/vinfo/us/security/definition/devops.
14. David Fiser. (March 4, 2020). *Trend Micro Research, News, and Perspectives.* "Security Risks in Online Coding Platforms." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/research/20/c/security-risks-in-online-coding-platforms.html.
15. Trend Micro. (May 14, 2020). *Trend Micro Security News.* "Cloud Security: Key Concepts, Threats, and Solutions." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/cloud-security-key-concepts-threats-and-solutions.
16. Melissa Clow. (Dec. 16, 2020). *Trend Micro Research, News, and Perspectives.* "A Guide to the Well-Architected Framework." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/devops/20/l/well-architected-framework-guide.html.
17. Trend Micro. (March 4, 2021). *Trend Micro Security News.* "Security 101: Virtual Patching." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-virtual-patching.
18. Trend Micro. (n.d.) *Trend Micro Security News.* "Ransomware Definition Page." Accessed on Nov. 8, 2021, at https://www.trendmicro.com/vinfo/us/security/definition/ransomware.

19. Trend Micro. (Sept. 28, 2017). *Trend Micro Security News.* "Spam, BEC, Ransomware: The Continuing Abuse of Email by Old and New Threats." Accessed on Nov. 8, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-spam-bec-ransomware-the-continuing-abuse-of-email-by-old-and-new-threats.
20. Dinesh Malkani. (June 4, 2021). *Forbes.* "Going Hybrid: The Future Of Work Is Here." Accessed on Nov. 8, 2021, at https://www.forbes.com/sites/forbestechcouncil/2021/06/04/going-hybrid-the-future-of-work-is-here/.
21. Trend Micro. (Sep. 14, 2021). *Trend Micro.* "Attacks From All Angles: 2021 Midyear Cybersecurity Report." Accessed on Nov. 19, 2021, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup.
22. Robert Lemos. (Oct. 27, 2021). *Dark Reading.* "Cybersecurity Talent Gap Narrows as Workforce Grows." Accessed on Nov. 22, 2021, at https://www.darkreading.com/careers-and-people/cybersecurity-talent-gap-narrows-as-workforce-grows.
23. Trend Micro. (June 8, 2021). *Trend Micro Security News.* "Modern Ransomware's Double Extortion and How to Protect Enterprises Against Them." Accessed on Nov. 19, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them.
24. Trend Micro. (April 14, 2020). *Trend Micro Security News.* "Undertaking Security Challenges in Hybrid Cloud Environments." Accessed on Nov. 8, 2021, at https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/undertaking-security-challenges-in-hybrid-cloud-environments.
25. Claudia Glover. (Oct. 11, 2021). *Tech Monitor.* "Ransomcloud: How and why ransomware is targeting the cloud." Accessed on Nov. 8, 2021, at https://techmonitor.ai/technology/cybersecurity/ransomcloud.
26. Patrick Howell O'Neill. (Sept. 23, 2021). *MIT Technology Review.* "2021 has broken the record for zero-day hacking attacks." Accessed on Nov. 5, 2021, at https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons.
27. Trend Micro. (July 13, 2021). *Trend Micro Security News.* "Trends and shifts in the underground N-day exploit market." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/trends-and-shifts-in-the-underground-n-day-exploit-market.
28. Trend Micro. (May 19, 2021). *Trend Micro Newsroom.* "Trend Micro's Zero Day Initiative Enhances Position as World's Largest Vulnerability Disclosure Player." Accessed on Nov. 25, 2021, at https://newsroom.trendmicro.com/2021-05-19-Trend-Micros-Zero-Day-Initiative-Enhances-Position-as-Worlds-Largest-Vulnerability-Disclosure-Player.
29. Clement Lecigne and Maddie Stone. (July 14, 2021). *Google.* "How we protect users from 0-day attacks." Accessed on Nov. 5, 2021, at https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks.
30. Jon Clay. (April 28, 2021). *Trend Micro Research, News, and Perspectives.* "How Trend Micro Helps Manage Exploited Vulnerabilities." Accessed on Dec. 3, 2021, at https://www.trendmicro.com/en_us/research/21/d/how-trend-micro-helps-manage-exploited-vulnerabilities.html.
31. Charlie Osborne. (July 14, 2021). *ZDNet.* "Microsoft July 2021 Patch Tuesday: 117 vulnerabilities, Pwn2Own Exchange Server bug fixed." Accessed on Nov. 5, 2021, at https://www.zdnet.com/article/microsoft-july-2021-patch-tuesday-117-vulnerabilities-pwn2own-exchange-server-bug-fixed.
32. Catalin Cimpanu. (Sept. 10, 2019). *ZDNet.* "Security researchers expose another instance of Chrome patch gapping." Accessed on Dec. 1, 2021, at https://www.zdnet.com/article/security-researchers-expose-another-instance-of-chrome-patch-gapping.
33. Trend Micro. (April 7, 2021). *Trend Micro Research, News, and Perspectives.* "The Nightmares of Patch Management: The Status Quo and Beyond." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond.
34. Magno Logan. (Oct. 8, 2021). *Trend Micro Security News.* "Minding the Gaps: The State of Vulnerabilities in Cloud Native Applications." Accessed on Nov. 17, 2021, at https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/minding-the-gaps-the-state-of-vulnerabilities-in-cloud-native-applications.
35. Shaun Nichols. (Nov. 2, 2021). *TechTarget.* "Why cloud bugs don't get CVEs, and why it's an issue." Accessed on Nov. 17, 2021, at https://searchsecurity.techtarget.com/news/252508948/Why-cloud-bugs-dont-get-CVEs-and-why-its-an-issue.
36. Trend Micro. (March 4, 2021). *Trend Micro Research.* "Security 101: Virtual Patching." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-virtual-patching.
37. Trend Micro. (Aug. 28, 2018). *AP News.* "Trend Micro Report Reveals Criminals Increasingly Drawn To Low-Profile Attacks." Accessed on Nov. 5, 2021, at https://apnews.com/press-release/pr-businesswire/7f2907b6661b426c855e4875511266e1.

38. BSI Staff. (July 26, 2021). *The British Standards Institution.* "How your business can adapt to cybersecurity trends." Accessed on Nov. 21, 2021, at https://shop.bsigroup.com/articles/how-your-business-can-adapt-to-cybersecurity-trends.
39. David Agranovich and Mike Dvilyanski. (Nov. 16, 2021). *Meta.* "Taking Action Against Hackers in Pakistan and Syria." Accessed on Nov. 21, 2021, at https://about.fb.com/news/2021/11/taking-action-against-hackers-in-pakistan-and-syria.
40. VMWare. (Oct. 11, 2021). VMWare Security Blog. "Moving Left of the Ransomware Boom." Accessed on Nov. 25, 2021, at https://blogs.vmware.com/security/2021/10/moving-left-of-the-ransomware-boom.html.
41. Lucian Constantin. (March 19, 2021). *CSO Online.* "Ryuk ransomware explained: A targeted, devastatingly effective attack." Accessed on Nov. 25, 2021, at https://www.csoonline.com/article/3541810/ryuk-ransomware-explained-a-targeted-devastatingly-effective-attack.html.
42. Jaromir Horejsi and Daniel Lunghi. (Sept. 13, 2021). *Trend Micro Research, News, and Perspectives.* "APT-C-36 Updates Its Spam Campaign Against South American Entities With Commodity RATs." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html.
43. National Cyber Security Centre. (Oct. 6, 2016). *National Cyber Security Centre.* "Common Cyber Attacks: Reducing The Impact." Accessed on Nov. 21, 2021, at https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact.
44. Trend Micro. (n.d.). *Trend Micro Security News.* "Ransomware Definition." Accessed on Nov. 21, 2021, at https://www.trendmicro.com/vinfo/us/security/definition/ransomware.
45. Numaan Huq et al. (June 28, 2019). *Trend Micro Research.* "Crimeware for Sale: The Commoditization of ATM Malware in the Cybercriminal Underground." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/crimeware-for-sale-the-commoditization-of-atm-malware-in-the-cybercriminal-underground.
46. Lawrence Abrams. (Nov. 15, 2021). *BleepingComputer.* "Emotet malware is back and rebuilding its botnet via TrickBot." Accessed on Nov. 22, 2021, at https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot.
47. Bernadette Caraig. (n.d.). *Trend Micro Threat Encyclopedia.* "The ZeuS, ZBOT, and Kneber Connection." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/16/the-zeus-zbot-and-kneber-connection.
48. Joshua Yaffa. (May 23, 2021). *The New Yorker.* "How Hacking Became a Professional Service in Russia." Accessed on Nov. 21, 2021, at https://www.newyorker.com/news/news-desk/how-hacking-became-a-professional-service-in-russia.
49. Catalin Cimpanu. (Jan. 19, 2021). *ZDNet.* "New FreakOut botnet targets Linux systems running unpatched software." Accessed on Nov. 5, 2021, at https://www.zdnet.com/article/new-freakout-botnet-targets-linux-systems-running-unpatched-software/.
50. Trend Micro. (n.d.). *Trend Micro Security News.* "Machine Learning." Accessed on Nov. 22, 2021, at https://www.trendmicro.com/vinfo/us/security/definition/machine-learning.
51. Gartner. (May 17, 2021). *Gartner.* "Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021." Accessed on Nov. 22, 2021, at https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem.
52. Bharath Aiyer, Venky Anant, and Daniele Di Mattia. (March 24, 2021). *McKinsey.* "Securing small and medium-size enterprises: What's next?" Accessed on Nov. 22, 2021, at https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/securing-small-and-medium-size-enterprises-whats-next.
53. Trend Micro. (May 28, 2020). *Trend Micro Security News.* "Smart Yet Flawed: IoT Device Vulnerabilities Explained." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/smart-yet-flawed-iot-device-vulnerabilities-explained.
54. Trend Micro. (July 22, 2021). *Trend Micro Security News.* "IoT Security Issues, Threats, and Defenses." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses.
55. Trend Micro. (Oct. 11, 2021). *Trend Micro Research, News, and Perspectives.* "Honda to Start Selling Smart Car Data." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/j/honda-to-start-selling-smart-car-data.html.
56. Kotaro Abe and Ryotaro Yamada. (Sept. 29, 2021). *Nikkei Asia.* "Honda joins $400bn gold rush to monetize smart car data." Accessed on Nov. 5, 2021, at https://asia.nikkei.com/Business/Technology/Honda-joins-400bn-gold-rush-to-monetize-smart-car-data.
57. Anthony Spadafora. (Nov. 18, 2020). *TechRadar.* "Amazon and NXP team up on smart car cloud computing deal." Accessed on Nov. 17, 2021, at https://www.techradar.com/news/amazon-and-nxp-team-up-on-smart-car-cloud-computing-deal.

58. Mark Minevich. (July 13, 2020). *Forbes.* "The Automotive Industry And The Data Driven Approach." Accessed on Nov. 5, 2021, at https://www.forbes.com/sites/markminevich/2020/07/13/the-automotive-industry-and-the-data-driven-approach/.
59. Toyota Motor Corporation. (Aug. 10, 2017). *Toyota Motor Corporation.* "Industry leaders to form consortium for network and computing infrastructure of automotive big data." Accessed on Nov. 5, 2021, at https://global.toyota/en/detail/18135029.
60. Numaan Huq, Craig Gibson, Vladimir Kropotov, and Rainer Vosseler. (Feb. 16, 2021). *Trend Micro Research.* "In Transit, Interconnected, At Risk: Cybersecurity Risks of Connected Cars." Accessed on Nov. 17, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars.
61. Trend Micro. (Feb. 6, 2021). *Trend Micro Research, News, and Perspectives.* "Connected Cars, 5G, the Cloud: Opportunities and Risks." Accessed on Nov. 17, 2021, at https://www.trendmicro.com/en_us/research/21/b/connected-cars-5g-the-cloud-opportunities-and-risks.html.
62. MIH Consortium. (Oct. 20, 2021). *MIH Consortium.* "MIH Unveils Open EV Software Platform and Announces key partnerships with Arm, Microsoft and Trend Micro." Accessed on Nov. 5, 2021, at https://www.mih-ev.org/en/news-info/?id=695.
63. Microsoft. (Feb. 10, 2021). *Microsoft News Center.* "Volkswagen Group teams up with Microsoft to accelerate the development of automated driving." Accessed on Nov. 17, 2021, at https://news.microsoft.com/2021/02/10/volkswagen-group-teams-up-with-microsoft-to-accelerate-the-development-of-automated-driving.
64. Garth Friesen. (Sep. 3, 2021). *Forbes.* "No End In Sight For The COVID-Led Global Supply Chain Disruption." Accessed on Nov. 25, 2021, at https://www.forbes.com/sites/garthfriesen/2021/09/03/no-end-in-sight-for-the-covid-led-global-supply-chain-disruption/.
65. Elizabeth Harris. (Oct. 4, 2021). *The New York Times.* "'The Beginning of the Snowball': Supply-Chain Snarls Delay Books." Accessed on Nov. 25, 2021, at https://www.nytimes.com/2021/10/04/books/book-publishing-supply-chain-delays.html.
66. Peter S. Goodman and Niraj Chokshi. (June 1, 2021). *The New York Times.* "How the World Ran Out of Everything." Accessed on Nov. 25, 2021, at https://www.nytimes.com/2021/06/01/business/coronavirus-global-shortages.html.
67. Trend Micro Research. (Jan. 26, 2021). *Trend Micro Research, News, and Perspectives.* "Examining A Sodinokibi Attack." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html.
68. Michael Novinson. (April 23, 2021). *CRN.* "Apple Menaced After REvil Ransomware Attack Against Supplier." Accessed on Nov. 5, 2021, at https://www.crn.com/news/security/apple-menaced-after-revil-ransomware-attack-against-supplier.
69. Trend Micro Research. (May 12, 2021). *Trend Micro Research, News, and Perspectives.* "What We Know About the DarkSide Ransomware and the US Pipeline Attack." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html.
70. Trend Micro Research. (July 4, 2021). *Trend Micro Research, News, and Perspectives.* "IT Management Platform Kaseya Hit With Sodinokibi/REvil Ransomware Attack." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/g/it-management-platform-kaseya-hit-with-sodinokibi-revil-ransomwa.html.
71. Janus Agcaoili et al. (June 15, 2021). *Trend Micro Security News.* "Ransomware Double Extortion and Beyond: REvil, Clop, and Conti." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.
72. Trend Micro. (Sept. 14, 2021). *Trend Micro.* "Attacks From All Angles: 2021 Midyear Cybersecurity Report." Accessed on Nov. 25, 2021, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup.
73. Brian Krebs. (May 11, 2021). *Krebs On Security.* "A Closer Look at the DarkSide Ransomware Gang." Accessed on Nov. 25, 2021, at https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/.
74. Chad P. Bown and Douglas A. Irwin. (Oct. 14, 2021). *The New York Times.* "Why Does Everyone Suddenly Care About Supply Chains?" Accessed on Nov. 6, 2021, at https://www.nytimes.com/2021/10/14/opinion/supply-chain-america.html.
75. Trend Micro. (Aug. 13, 2021). *Trend Micro Research, News, and Perspectives.* "What Is Zero Trust and Why Does It Matter?" Accessed on Nov. 9, 2021, at https://www.trendmicro.com/en_us/ciso/21/h/what-is-zero-trust-and-why-does-it-matter.html.

VERSO UN NUOVO SLANCIO

LE PREVISIONI SULLA SICUREZZA DI TREND MICRO PER IL 2022

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 e con una propensione all'innovazione continua, Trend Micro protegge centinaia di migliaia di organizzazioni e milioni di individui che utilizzano il cloud, le reti e i più diversi dispositivi, attraverso la sua piattaforma di cybersecurity.

Trend Micro è leader nelle soluzioni di sicurezza cloud ed enterprise e la sua piattaforma abilita una vasta gamma di tecniche avanzate di difesa dalle minacce, che sono ottimizzate per gli ambienti AWS, Microsoft e Google. La piattaforma Trend Micro consente anche di avere una visibilità centralizzata, per usufruire di un rilevamento e risposta migliori e più rapidi.

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