Previsioni Trend Micro sulla sicurezza per il 2020

TREND MICRO™ | research

IL FUTURO È COMPLESSO

Pag. 4

ESPOSTO

Pag. 9

MAL CONFIGURATO

Pag. 13

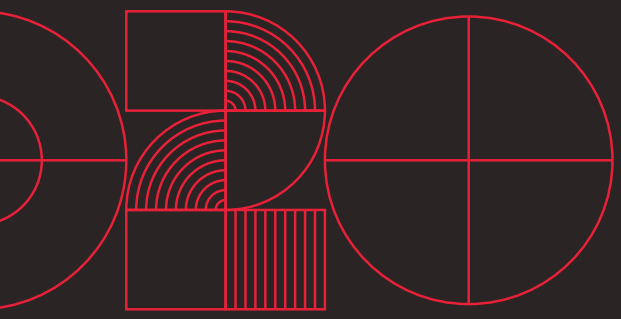
DIFENDIBILE

Pag. 17

CYBERSECURITY NEL 2020

Pag. 20

Pubblicato da Trend Micro Research
Immagini d'archivio: Shutterstock.com



LA NUOVA NORMALITÀ

Previsioni Trend Micro sulla sicurezza per il 2020

Come l'anno 2020 segna l'arrivo di un nuovo decennio, così recenti eventi e tendenze indicano una svolta altrettanto significativa nello scenario delle minacce. Dal 2020 in poi la cybersecurity dovrà essere osservata attraverso numerose lenti – dalle diverse motivazioni degli attaccanti e degli arsenali dei cybercriminali fino agli sviluppi tecnologici e all'intelligence globale sulle minacce – affinché le difese possano tenere testa e anticipare tanto i player tradizionali e quelli più innovativi quanto i nuovi arrivati.

Il vecchio paradigma che prevedeva l'isolamento delle reti dietro a un firewall aziendale è ormai un ricordo. Non sono più i tempi in cui si utilizzava uno stack limitato di applicazioni enterprise. Il paradigma attuale prevede al contrario un'ampia gamma di app, servizi e piattaforme che richiede inevitabilmente di essere protetta. Una sicurezza stratificata da applicare alle diverse implementazioni e capace di tenere il passo con i cambiamenti dell'ecosistema si rivelerà essenziale per affrontare tutte le minacce che ci attendono.

Metodi ormai rodati come estorsioni, offuscamenti e phishing continuano ad avere successo negli attacchi che osserviamo oggi, ma è inevitabile che emergano nuovi rischi. Il continuo spostamento verso il cloud, per esempio, non fa che accentuare l'eventuale errore umano: una configurazione sbagliata contribuisce alla possibilità di compromettere l'ambiente in maniera esponenziale. Il solo numero di infrastrutture e asset connessi dà vita a un'ulteriore insieme di problemi che apre le porte alle minacce. Non meno complesse saranno le minacce rivolte contro le aziende, con attacchi condotti mediante un mix di tecniche tradizionali e nuove tecnologie, come l'intelligenza artificiale (AI).

Le previsioni Trend Micro sulla sicurezza per il 2020 riflettono le opinioni e le analisi dei nostri esperti sul tema delle tecnologie e delle minacce emergenti. Gli scenari e gli sviluppi descritti appartengono a un futuro possibile nel quale il progresso tecnologico e l'evoluzione delle minacce saranno fattori determinanti per i cambiamenti di scenario. Questo report intende offrire alle aziende gli strumenti utili per prendere decisioni informate su specifiche aree della sicurezza, che saranno interessate da sfide e opportunità nel 2020 ma anche nei decenni che seguiranno.

IL FUTURO È COMPLESSO

Il modo in cui il panorama delle minacce si è evoluto negli anni dimostra come i cybercriminali proseguano imperterriti nel compromettere sistemi per il proprio tornaconto. Per questo, si adattano e cambiano costantemente tattiche e vettori di attacco, imponendo a utenti e aziende di restare al passo.

Gli attaccanti sono più rapidi di patch incomplete e frettolose.

Gli amministratori di sistema dovranno prestare cautela quando si tratta non solo della tempestività con cui applicano le patch, ma anche della qualità delle medesime patch. Applicare una patch di scarsa qualità a un sistema critico potrebbe provocare problemi a funzionalità importanti o un blocco dovuto ai difetti della patch stessa. D'altra parte, anche ritardare l'installazione di una patch mette un sistema a rischio di compromissione, causato da un attacco che può sfruttare una vulnerabilità nota.

Problematiche collegate alle patch lasciano aperte finestre di esposizione che gli attaccanti useranno come punti di ingresso. Prevediamo un aumento dei casi di aggiramento delle patch dovuti a carenze di quest'ultime. Per esempio, un attaccante può sfruttare un exploit cambiando un paio di righe di codice alla fix. Ad esempio, lo scorso anno si era scoperto che una patch creata per una vulnerabilità zero-day di JET Database Engine era "incompleta", ovvero limitava ma non eliminava il difetto[1]. Nel 2019 gli hacker hanno sfruttato vulnerabilità presenti nei router Cisco, che sono state risolte solo parzialmente dalle relative fix[2].

Gli attaccanti faranno affidamento sul fatto che gli utilizzatori di librerie open source trascureranno le fix rilasciate dai relativi maintainer; inoltre sfrutteranno il cosiddetto patch gapping, un metodo che approfitta di una vulnerabilità prima che la relativa patch venga rilasciata agli utenti di quei prodotti che utilizzano una libreria vulnerabile[3].

Nei casi in cui la patch non neutralizzi la vulnerabilità o esista un gap nell'implementazione della patch stessa, il virtual patching può essere d'aiuto fornendo protezione immediata e facendo da schermo contro vulnerabilità note e ignote.

I cybercriminali utilizzeranno le piattaforme blockchain per le transazioni clandestine.

L'ecosistema underground continuerà a evolvere seguendo l'ulteriore proliferazione delle attività cybercriminali. La fiducia ricoprirà un ruolo importante nei mercati clandestini, come prova per l'implementazione di sistemi di controllo preventivo e pagamenti nelle transazioni ad alto rischio[4]. La blockchain diventerà un nuovo mezzo per stabilire un sistema di fiducia distribuito tra acquirenti e venditori; gli smart contract permetteranno ai cybercriminali di formalizzare i pagamenti tramite criptovalute e registrarli nella blockchain. Per mantenere l'anonimato e ridurre il rischio di exit scam, i cybercriminali si rivolgeranno a mercati basati su blockchain che offrono un sistema decentralizzato per le transazioni[5].

Malware ormai tradizionale, come il ransomware e il modello di business crime-as-a-service, continueranno a rappresentare opzioni immancabili per quei cybercriminali alla ricerca di un facile profitto.

I sistemi bancari saranno nel mirino con open banking e malware per bancomat.

Nel 2020 assisteremo all'incremento degli operatori di malware mobile specializzato nell'attacco contro i sistemi per i servizi bancari e i pagamenti online. In Europa cresceranno i pagamenti online all'aumentare del numero di banche che confermeranno il proprio supporto a questo tipo di pagamenti[6]. Con la seconda direttiva sui servizi di pagamento (PSD2) ora in vigore nell'Unione Europea e con altri Paesi che presto seguiranno con le rispettive normative[7], non siamo molto lontani dalla diffusione dei servizi di "open banking". Ciò comporta tuttavia diverse implicazioni in più per la sicurezza del paradigma bancario, dai difetti nelle API bancarie alle nuove strategie messe a punto per le campagne di phishing[8]. Vecchi e nuovi player del settore dovranno adottare misure che vanno dallo sviluppo di software intrinsecamente sicuro, fino allo svolgimento di audit di sicurezza regolari.

La trasformazione in commodity del crimeware, per l'attacco agli sportelli bancomat, conquisterà ulteriore terreno. Varianti di Cutlet Maker, Hello World e WinPot sono già in vendita. Ci aspettiamo che queste famiglie di malware dedicati ai bancomat competano per il predominio negli ambienti underground[9].

Deepfake, la nuova frontiera delle frodi contro le aziende.

Per anni, le truffe veicolate attraverso le email con tecniche che si sono evolute nel tempo[10], sono state diffuse principalmente[11] da malviventi dell'Africa occidentale, e non ci aspettiamo che questa situazione cambi. Per il 2020 prevediamo ulteriori sviluppi di queste frodi per mezzo delle nuove tecnologie, in particolare dell'intelligenza artificiale (AI). La AI viene utilizzata per creare contenuti contraffatti (immagini, video o audio) altamente credibili in cui determinate persone dicono o fanno cose in realtà mai avvenute: sono quelli che vengono chiamati "deepfake"[12]. La diffusione dei deepfake è preoccupante, poiché inevitabilmente varia dalla creazione di finti video pornografici con persone famose alla manipolazione di dipendenti e procedure aziendali.

L'utilizzo da parte dei cybercriminali di contenuti vocali generati dall'intelligenza artificiale a scopo di social engineering, è stato rilevato per la prima volta nel 2019. A quanto riferito, un'azienda elettrica sarebbe stata derubata di 243.000 dollari da truffatori che avrebbero usato una AI per imitare la voce del CEO della società[13]. Ulteriori tentativi del genere sfrutteranno la tecnologia per creare deepfake di responsabili e manager nel tentativo di convincere qualche dipendente a trasferire fondi o prendere decisioni critiche. Si assisterà a un'evoluzione che abbandonerà le tradizionali campagne BEC (Business Email Compromise) e le truffe dei finti servizi di supporto tecnico. I malviventi non si affideranno più esclusivamente alla falsificazione degli indirizzi email ma approfitteranno dell'elemento audiovisivo dei deepfake per rendere maggiormente credibili i loro messaggi. Gli alti manager delle aziende costituiranno l'obiettivo principale di questo genere di frodi dal momento che compaiono spesso in call, conferenze, media e video online[14].

Google ha già rilasciato un enorme dataset di video deepfake per aiutare i ricercatori a rilevare le falsificazioni[15]. Anche se le "truffe da deepfake" possono essere ancora nelle loro fasi iniziali, i dipendenti delle aziende dovranno subito imparare a identificare i segnali rivelatori dei deepfake: per esempio difformità nell'intonazione, lentezza del parlato e aspetto artificiale della pelle nei video. Sarà poi essenziale adottare ulteriori passaggi di verifica nei processi di natura finanziaria.

I Managed Service Provider saranno colpiti per distribuire malware e scatenare attacchi supply chain.

Le aziende si affidano sempre più all'outsourcing per le proprie attività ed esigenze quotidiane. Da qui nasce il pericolo che attacchi supply chain possano aggirare e mettere a repentaglio i processi di business[16] e le misure di sicurezza. Il rischio risiede nel concedere fiducia assoluta a terze parti come i Managed Service Provider (MSP).

Negli anni gli attacchi supply chain hanno assunto numerose forme, dal prendere il controllo degli aggiornamenti software al compromettere i servizi di terze parti per colpire le aziende con codice dannoso[17]. Quest'ultima modalità è quella che prevediamo possa colpire prevalentemente le PMI nel corso del 2020. Se una PMI affida porzioni delle proprie infrastrutture o delle proprie operazioni in outsourcing, i fornitori esterni possono diventare il trampolino da cui lanciare attacchi.

Una violazione della supply chain di un MSP può diffondersi a cascata ad altri soggetti. I malviventi attaccheranno i service provider per caricare codice dannoso nei loro siti allo scopo di raccogliere, tra l'altro, i dati sensibili dei clienti. Gli attaccanti troveranno distributori o fornitori con livelli di sicurezza insufficiente per diffondere il malware ai loro clienti. Per esempio, una violazione nell'infrastruttura di un produttore di software ha permesso a un hacker di installare ransomware su centinaia di sistemi per la gestione degli studi dentistici[18]. Questa tendenza è destinata a proseguire, se non addirittura ad accelerare.

Per evitare di essere colpiti da attacchi di questo genere bisognerebbe condurre regolarmente valutazioni delle vulnerabilità e dei rischi predisponendo misure preventive come una verifica approfondita dei provider e dei dipendenti che possono accedere ai sistemi.

Gli attaccanti approfitteranno dei bug trasformabili in worm e deserializzazione.

In maggio Microsoft ha rilasciato una fix per una vulnerabilità RCE (Remote Code Execution) critica, designata CVE-2019-0708 e soprannominata "BlueKeep". Da allora la società ha rilasciato aggiornamenti simili per altre vulnerabilità che colpiscono la componente Remote Desktop Services di Windows. Poiché queste vulnerabilità possono essere trasformate in worm, qualsiasi malware che ne approfittasse potrebbe diffondersi tanto velocemente quanto WannaCry, che si era propagato rapidamente in tutto il mondo bloccando centinaia di migliaia di sistemi informatici. Lo sviluppo di un exploit in grado di sfruttare BlueKeep è tuttavia questione complessa che richiede un livello di know-how tecnico davvero elevato. Per esempio, un modulo Metasploit che implementa questa vulnerabilità è stato sì rilasciato, ma a differenza di EternalBlue si è dimostrato poco pratico[19].

Sentiremo ancora parlare di BlueKeep, e i tentativi di sfruttare altre vulnerabilità gravi non mancheranno certamente. Protocolli largamente utilizzati come SMB (Server Message Block) e RDP (Remote Desktop Protocol) saranno oggetto di attenzione da parte di chi desidera penetrare all'interno di sistemi non protetti. Il protocollo SMB è già stato notoriamente usato per veicolare gli exploit WannaCry e NotPetya. Anche il protocollo RDP non è rimasto immune a problematiche di sicurezza: oltre a essere utilizzato per far funzionare BlueKeep, è anche un comune vettore di ingresso per il ransomware. Non a caso i responsabili del ransomware SamSam vanno alla ricerca di dispositivi che hanno connessioni RDP esposte[20].

Altre vulnerabilità che prevediamo possano diventare un'importante fonte di preoccupazione per le aziende riguardano i bug di deserializzazione. Gli errori che comportano la deserializzazione dei dati non verificati rappresentano una classe di vulnerabilità altamente critica che, rivolta contro le applicazioni enterprise, è in grado di modificare oggetti o dati ritenuti immuni da mutamenti[21]. La serializzazione è una tecnica usata da molti linguaggi di programmazione per tradurre un oggetto in un formato adatto a essere memorizzato o trasmesso. La deserializzazione è l'esatto processo contrario. Uno dei rischi riguarda il modo in cui le applicazioni che accettano oggetti serializzati non convalidano i dati in ingresso prima di *deserializzarli*. Attaccanti particolarmente abili possono cercare di sfruttare questo comportamento, inserendo un oggetto dannoso all'interno di un flusso di dati, per poi farlo eseguire dall'app server.

Anziché concatenare un certo numero di vulnerabilità per arrivare a far eseguire il proprio codice, gli attaccanti possono sfruttare i bug di deserializzazione per ottenere il controllo completo da remoto ed eseguire il codice automaticamente, anche all'interno di ambienti complessi. La serializzazione e la deserializzazione sono concetti importanti nelle applicazioni Java e riguardano un gran numero di applicazioni web e prodotti middleware. Le aziende che usano piattaforme che supportano questi meccanismi dovrebbero applicare immediatamente patch e virtual patch[22], oltre che diventare consapevoli del grado di vulnerabilità dei sistemi o del software che possiedono.

Il futuro convergente apre la strada ad attacchi e tecniche di vecchia e di nuova concezione, che lasciano esposti asset IT (Information Technology) e OT (Operational Technology).

I cybercriminali sfrutteranno i dispositivi IoT a scopo di spionaggio ed estorsione.

Prevediamo che i cybercriminali utilizzeranno machine learning e AI per l'ascolto dei dispositivi connessi in ambienti enterprise, come per esempio smart TV e smart speaker. In questo modo potranno sfruttare le tecniche di riconoscimento del linguaggio e identificazione degli oggetti per carpire conversazioni personali e di lavoro; da qui potranno identificare possibili obiettivi per estorsioni o conquistare una base per attività di spionaggio industriale.

Come per altre forme di monetizzazione degli attacchi IoT, i cybercriminali devono ancora trovare un modello di business scalabile in grado di sfruttare l'ampia superficie di attacco offerta dall'IoT e dai mutamenti di scenario come le reti 5G. La monetizzazione degli attacchi IoT, pur essendo ancora agli albori, sarà sperimentata dai cybercriminali in diversi modi. Le estorsioni digitali[23] rappresentano il metodo più probabile.

Nelle community underground i cybercriminali discutono spesso di come compromettere varie tipologie di dispositivi connessi per i loro scopi illeciti. Le tecniche di violazione vengono provate innanzitutto sui dispositivi consumer, mentre le apparecchiature industriali connesse costituiscono l'obiettivo successivo. Abbiamo già osservato discussioni inerenti le schede PLC (Programmable Logic Controller) che vengono adoperate per controllare apparati di produzione industriale su larga scala.

I dispositivi IoT come i router verranno monetizzati per mezzo di botnet che potranno essere successivamente impiegate come reti distribuite per i servizi offerti ai cybercriminali. Non è azzardato prevedere che l'hacking dei router venga effettuato anche sotto forma di botnet per il dirottamento dei servizi DNS (Domain Name Server), implementato come crimeware piuttosto che come servizio, principalmente a scopo di phishing. Altre proposte veicolate negli ambienti underground riguardano l'accesso agli stream video di webcam e a contatori intelligenti dotati di firmware modificato. Tutto questo stimolerà sempre più la discussione sulla sicurezza IoT, in particolare sul fatto che non tutti i dispositivi IoT possiedono misure di sicurezza né sono equipaggiati per difendersi dalla varietà di attacchi che registriamo oggi.

Gli utenti 5G saranno alle prese con le implicazioni di sicurezza che il passaggio alle reti software-defined comporta.

Con il diffondersi del 5G nel 2020, ci aspettiamo l'arrivo di diverse vulnerabilità. Nonostante l'automazione, le difficoltà saranno causate da inevitabili difetti del codice, ma anche perché i produttori non saranno sufficientemente preparati ad affrontare le minacce relative a questa tecnologia.

Dal momento che l'ambiente 5G non è altro che una rete di tipo software-defined, che offre a utenti e dispositivi una connettività ad alta bandwidth e bassa latenza, è prevedibile che le reti di questo genere serviranno un'ampia varietà di applicazioni e settori verticali. Le minacce collegate alle reti 5G scaturiranno da operazioni software vulnerabili (per esempio, una rete 5G gestita da un software o da un fornitore potenzialmente vulnerabile) e dal fatto che sono reti molto distribuite (maggiori possibilità di attacco - numero dei dispositivi IoT connessi). Gli attaccanti cercheranno di assumere il controllo del software che gestisce le reti 5G allo scopo di controllare la rete stessa. Anche gli aggiornamenti relativi al 5G somiglieranno molto agli aggiornamenti software degli smartphone e comporteranno vulnerabilità[24]. I ricercatori hanno già dimostrato come le vulnerabilità del 5G possano essere sfruttate in diversi modi usando piattaforme hardware e software a basso cost[25] ed è logico presumere che i cybercriminali non siano molto distanti dal fare lo stesso. L'assenza di sicurezza nelle reti 5G peggiorerà le potenziali minacce inerenti alla confidenzialità (per esempio lo spionaggio di dati e traffico), all'integrità (per esempio la modifica dei dati trasmessi) e alla disponibilità (per esempio i malfunzionamenti di rete che colpiscono settori interdipendenti)[26].

La misura del successo di nazioni e operatori sembra attualmente quella di chi riesce a implementare il 5G per primo, sacrificando la sicurezza sull'altare della rapidità. Pensare alla sicurezza del 5G solo in un secondo tempo, a causa di migrazioni affrettate e configurazioni carenti, provocherà difficoltà specialmente nel momento in cui aumenteranno i servizi dipendenti dalla rete. Aggiungere la sicurezza alle infrastrutture 5G successivamente al loro deployment sarà più complesso che non includerla fin dall'inizio[27]. Mitigare le conseguenze di protezioni inadeguate richiederà professionisti della sicurezza capaci di identificare i problemi specifici delle reti software-defined[28]. Se le funzioni di rete sono dinamiche, allora anche la sicurezza deve esserlo. Per esempio, nel deployment dinamico dei servizi di rete per mezzo di NFV (Network Functions Virtualization) e virtualizzazione applicativa, la sicurezza deve essere capace anche di tenere il ritmo della rapidità di implementazione delle applicazioni.

Le infrastrutture critiche saranno ancora più colpite da attacchi e interruzioni operative.

Utility e altre infrastrutture critiche (CI) continueranno a rappresentare obiettivi appetibili a scopo di estorsione anche nel 2020. Il ransomware sarà ancora l'arma preferita dal momento che il rischio per le aziende è elevato: interruzioni operative prolungate si traducono infatti in pesanti perdite finanziarie e le linee di produzione possono essere messe in ginocchio per settimane a seconda di quanto tempo occorre per riuscire a ripristinare i sistemi. Gli attaccanti possono inoltre assemblare botnet per scatenare attacchi DDoS (Distributed Denial of Service) contro le reti OT (Operational Technology). Le industrie che si avvalgono di cloud service provider correranno il rischio di subire attacchi supply chain; i provider poco protetti potrebbero diventare i punti di partenza da cui attaccare e immobilizzare la produzione. I cyberattacchi mettono a repentaglio la disponibilità (un elemento prioritario all'interno di queste infrastrutture) e la pressione per rafforzare la cybersicurezza delle aziende che si avvalgono di ambienti IIoT (Industrial Internet of Things) è destinata a crescere[29].

Durante gli scorsi anni differenti autori di minacce hanno messo nel mirino diversi impianti di energia in tutto il mondo, nel corso di campagne di ricognizione. Queste attività legate ad attacchi ransomware mirati hanno lo scopo di ottenere le credenziali dei sistemi di controllo industriale (ICS) e dei sistemi SCADA (Supervisory Control And Data Acquisition) e carpire le informazioni relative alle modalità di funzionamento di questi impianti. L'impatto di queste violazioni non si propaga solamente al sistema CI colpito ma anche a quelli interdipendenti, provocando conseguenze diffuse (come il fermo delle centrali elettriche locali e l'interruzione delle forniture elettriche[30]).

Il blocco dei sistemi provocato da attacchi non riguarda solamente le utility. La produzione alimentare, i trasporti e l'industria sono altri comparti a rischio, considerando il crescente utilizzo di applicazioni IoT e interfacce uomo-macchina (HMI), come perno principale per la gestione di moduli diagnostici e di controllo in questi settori.

Le CI e le infrastrutture IT degli enti pubblici si troveranno esposte ad attacchi per periodi più lunghi rispetto a quelli degli ambienti industriali privati, dal momento che queste aree del settore pubblico tendono a essere sottofinanziate. Le informazioni raccolte durante le campagne di ricognizione offriranno ai malintenzionati l'opportunità di condurre attacchi maggiormente coordinati non solo per bloccare le infrastrutture, ma anche i servizi pubblici e i processi della politica.

Gli ambienti home office e di lavoro da remoto ridefiniranno gli attacchi supply chain.

Le aziende dovranno prestare attenzione ai rischi introdotti dagli accordi inerenti al lavoro da casa e dai dispositivi domestici connessi a Internet, che di fatto rendono indistinto il confine della sicurezza aziendale. Dopo tutto, lavorare da casa non è altrettanto sicuro come farlo dall'interno della rete corporate. Una sicurezza Wi-Fi carente, poi, aumenta il rischio del lavoro da remoto condotto in spazi pubblici o condivisi. Una rete aperta lascia esposti file e dati sensibili che possono essere raggiunti da altri utenti collegati alla medesima rete[31]. I dispositivi remoti possono essere infettati da malware che entra nella rete aziendale, per poi sottrarre informazioni di valore.

La moderna forza lavoro mobile non è più vincolata a un computer situato all'interno di un ufficio tradizionale. Rispetto al modello BYOD (Bring Your Own Device), i dipendenti che lavorano da casa possono passare da un dispositivo connesso all'altro per accedere a software di comunicazione e app residenti su cloud. I dispositivi domestici connessi che fungono da gateway per gli attacchi rivolti contro le aziende rappresentano un'evoluzione inevitabile, considerando quanti dipendenti possono trovare tali apparecchiature (smart TV, smart speaker e assistenti domestici) utili anche per il proprio lavoro. Le aziende dovranno decidere quali policy per la sicurezza delle informazioni implementare per affrontare scenari del genere.

Sfruttando il patrimonio di informazioni personali che hanno già ammassato, i cybercriminali predisporranno attacchi contro le aziende attraverso reti domestiche e pubbliche, impersonando i dipendenti. Questi attacchi sempre più sofisticati estenderanno la compromissione di processi ed email aziendali ben oltre il semplice dirottamento di fondi finanziari o infezioni di malware: l'ambiente domestico del dipendente diventerà il trampolino di lancio di attacchi supply chain.


MISCONFIGURATO
IL FUTURO È
MISCONFIGURATO
Le migrazioni verso gli ambienti cloud
e DevOps presentano sia vantaggi che rischi,
questo sottolinea l'esigenza di sicurezza
lungo tutta la catena del deployment

Le vulnerabilità dei container saranno la principale preoccupazione di sicurezza per i team DevOps.

Lo spazio dei container[32] si muove ad alta velocità. I rilasci sono rapidi, le architetture vengono integrate di continuo e nuove versioni del software escono con regolarità. Le pratiche di sicurezza tradizionali non saranno in grado di reggerne il ritmo.

Questo sottolinea l'importanza dei principi DevSecOps per i team DevOps dal momento che i container ribaltano un maggior numero di convenzioni e si fanno carico di un maggior numero di ruoli che per le aziende hanno natura critica. La rapidità dei cicli di sviluppo potrebbe lasciare poco margine per condurre test di sicurezza e vulnerabilità. Un'applicazione oggi può richiedere alle aziende di proteggere centinaia di container diffusi attraverso molteplici macchine virtuali residenti su piattaforme di servizi cloud differenti. Le aziende dovranno affrontare problematiche nei vari componenti dell'architettura a container, comprese le vulnerabilità presenti nei runtime (ad esempio Docker, CRI-O, Containerd e runC33), negli orchestratori (come Kubernetes) e negli ambienti di build (come Jenkins). Gli attaccanti troveranno la maniera di sfruttare qualsiasi anello debole capace di compromettere la catena DevOps.

Le vulnerabilità presenti all'interno delle immagini dei container ampiamente diffuse avranno un effetto nefasto sulla pipeline aziendale, nel momento in cui dovessero essere scaricate. L'applicazione di patch ai container si rivelerà particolarmente problematica per le aziende che si affidano a una terza parte per ottenere la relativa fix, dovendosi fidare del fatto che questa sia sicura. Le vulnerabilità presenti nelle applicazioni containerizzate colpiranno non solo il codice o l'engine del container ma anche numerosi altri elementi dello stack, che i cybercriminali potranno sfruttare a scopo di accesso e controllo.

Le piattaforme serverless aumenteranno la superficie di attacco a causa di errori di configurazione e codici vulnerabili.

Sempre più aziende adottano piattaforme serverless per integrare le applicazioni cloud e ridurre i costi. Gartner prevede che oltre il 20% delle aziende di tutto il mondo disporrà di tecnologie informatiche serverless entro il 2020[33]. Le piattaforme serverless offrono "funzioni as-a-service" permettendo agli sviluppatori di eseguire codice senza che l'azienda debba pagare per un intero server o container[34]. Tuttavia, essere serverless non significa essere immuni da problemi di sicurezza.

Ci aspettiamo che librerie obsolete, configurazioni errate e vulnerabilità note e ignote diventino punti di ingresso nelle applicazioni serverless da parte delle minacce. Gli attaccanti potranno quindi trarne vantaggio per raccogliere informazioni sensibili o penetrare nelle reti enterprise[35].

Le piattaforme serverless comprendono anche container e funzioni serverless oltre che altre dipendenze, sottolineando ulteriormente la complessità dalla quale potrebbe avere origine una minaccia. Dal momento che i sistemi serverless implementano le funzioni, specialmente quelle open source, in modalità stateless, il monitoraggio dei permessi e la memorizzazione dei dati sensibili costituiranno ulteriori preoccupazioni per tutto il 2020. Oltre all'aumento della visibilità di rete, anche il miglioramento dei processi e la documentazione dei workflow saranno essenziali per poter utilizzare applicazioni serverless.

Come accade per le applicazioni basate su container, le pratiche DevSecOps dovrebbero essere prioritarie anche nei deployment serverless. Gli ambienti serverless potranno trarre vantaggio anche dall'integrazione continua e dalla facilità d'utilizzo che rappresentano gli obiettivi di DevSecOps[36]. I tool per la sicurezza adatti alle infrastrutture serverless, comprese le dipendenze e le vulnerabilità delle applicazioni open source, saranno importanti per l'adozione di ambienti serverless e il deployment di funzioni specifiche.

Errori di configurazione da parte degli utenti e il coinvolgimento di terze parti non sicure, aumenteranno i rischi nelle piattaforme cloud.

Un'azienda può essere lo stesso a rischio nonostante l'aggiornamento regolare dei sistemi e la presenza di misure appropriate, qualora nel deployment vi siano applicazioni configurate erroneamente e problematiche di autenticazione. Controlli di sicurezza basilari che non siano implementati correttamente rappresenteranno un'enorme minaccia per la sicurezza dei dati di un'azienda.

Prevediamo un aumento degli incidenti relativi a reti compromesse, a causa di punti deboli dei servizi cloud. Gli errori di configurazione nel cloud storage che provocano la perdita di dati continueranno a essere un problema diffuso per le aziende anche nel 2020. Restrizioni insufficienti sull'accesso, errata gestione dei controlli sui permessi, negligenza nel logging delle attività e asset esposti pubblicamente sono solo alcuni dei passi falsi che le aziende compiono quando predispongono le loro reti cloud. Errori e guasti relativi ai servizi cloud lasciano esposti i dati delle aziende e possono portare anche a multe e sanzioni. Questi rischi potrebbero essere ridotti migliorando il profilo complessivo della sicurezza cloud (per esempio mediante la corretta configurazione e implementazione delle infrastrutture) e assicurando il rispetto di best practice e standard di settore.

Con il passaggio verso il cloud di aziende e impianti di produzione, come quelli industriali[37], aumenterà il coinvolgimento di service provider esterni. Esiste il rischio che questi vendor possano essere meno esperti di cloud di quanto dovrebbero (abituati ad esempio a processi e sistemi tradizionali) e non siano equipaggiati per proteggere l'infrastruttura. Gli attaccanti saranno motivati a lanciare attacchi DDoS mediante botnet contro i service provider per destabilizzare i servizi cloud.

Le piattaforme cloud saranno preda di attacchi a iniezione di codice attraverso librerie di terze parti.

Nel corso del 2020 aumenteranno le violazioni delle piattaforme cloud effettuate con attacchi a iniezione di codice, sia direttamente nel codice stesso che attraverso librerie di terze parti. L'iniezione di malware può servire a intercettare o assumere il controllo dei file e delle informazioni che un utente mantiene nel cloud. Forme comuni di questi attacchi diretti contro le applicazioni web dei servizi cloud sono gli attacchi XSS (cross-site scripting) e quelli di SQL injection. Un attacco di successo permette agli hacker di recuperare dati sensibili e manipolare i contenuti dei database a distanza. In alternativa gli attaccanti possono optare per una strada diversa agendo sulle librerie di terze parti che, una volta scaricate dagli utenti, mandano in esecuzione codice dannoso[38].

Nel frattempo ci aspettiamo che aumentino gli attaccanti che seguono i dati nel loro spostamento verso il cloud. Le violazioni del cloud sono prevedibili sulla scia della diffusione dei modelli di cloud computing di tipo software-as-a-service, infrastructure-as-a-service e platform-as-a-service. Più sono i dati corporate residenti nel cloud, più i malintenzionati sono interessati. Prevenire le violazioni del cloud richiederà debita diligenza da parte degli sviluppatori, la scrupolosa considerazione dei provider e delle piattaforme offerte, e il miglioramento della gestione della sicurezza del cloud.

IL FUTURO È DIFENDIBILE

Il gap nelle competenze di cybersecurity e la scarsa attenzione alla sicurezza sono le basi di una mancata protezione; la gestione del rischio e un'intelligence completa sulle minacce sono essenziali per creare un ambiente protetto.

Il rilevamento predittivo e comportamentale sarà essenziale contro le minacce persistenti e fileless.

Le minacce che vivono delle risorse che trovano continueranno a evadere le tradizionali tecniche di blacklisting. Le aziende dovranno considerare soluzioni complete di indicatori comportamentali, sandbox e monitoraggio del traffico. Dal momento che queste minacce si installano nel registro, risiedono nella memoria di un sistema o abusano di tool normalmente consentiti come PowerShell e Windows Management Instrumentation (WMI), il controllo di indicatori non basati su file come l'esecuzione di specifici comportamenti o eventi sarà importante ai fini del rilevamento. Le tecniche fileless continueranno a essere utili per altre forme di attacco che diffondono trojan bancari, malware per il mining di criptovalute e ransomware[39].

Oltre alle minacce Linux dedicate all'infezione dei dispositivi Internet of Things (IoT) allo scopo di farli diventare parte di botnet DDoS[40], anche il malware Linux conoscerà una crescita sostenuta dal momento che questo sistema open source sta diventando un componente importante, se non addirittura dominante[41], delle piattaforme enterprise. Ci aspettiamo che queste minacce persistano nei sistemi enterprise attraverso vari metodi, incluse le tecniche fileless, pronte a moltiplicare i propri processi per ulteriori attacchi

Il framework MITRE ATT&CK giocherà un ruolo crescente nella valutazione della sicurezza da parte delle aziende.

Il framework MITRE ATT&CK mette a disposizione una matrice completa per la valutazione della sicurezza. La sua knowledge base pubblica utilizza attacchi noti per classificare e spiegare le tattiche e le tecniche avversarie[42]. Prevediamo che sempre più aziende osservino i modelli di minaccia, i prodotti per la sicurezza e i rischi organizzativi attraverso la lente di questo framework. A parte i cacciatori di minacce che possono ottenere una miglior comprensione in merito ai vari attacchi e ai relativi pattern, anche chi deve difendersi potrà trarne beneficio misurando l'efficacia delle proprie tecniche di mitigazione e dei tool per la sicurezza utilizzati. La knowledge base MITRE ATT&ACK può essere una risorsa comune per i responsabili della sicurezza e i provider di cybersecurity, razionalizzando il modo di condividere l'intelligence sulle tecniche degli attaccanti e sulle misure difensive.

L’intelligence sulle minacce dovrà essere potenziata con competenze di analytics mirate, per proteggere i vari layer della sicurezza.

Pensiamo che dal 2020 in poi gli attacchi verranno pianificati, diffusi e diversificati in termini tattici in modo più accurato. L’intelligence sulle minacce e le analisi della sicurezza aiuteranno le aziende a difendere i propri ambienti identificando i gap di sicurezza, eliminando gli anelli deboli e permettendo di capire le strategie degli attaccanti. Una completa intelligence sulle minacce, inserita nei processi di sicurezza e relativa gestione del rischio, si rivelerà assolutamente preziosa per le aziende che intendono mitigare i rischi prima che possa verificarsi un qualsiasi attacco.

Le violazioni condotte per mezzo di minacce avanzate, malware persistente, normale phishing, potenziali zero-day e altri attacchi possono essere evitate qualora siano disponibili insight e protezioni. Possedere una visibilità completa sull’ambiente permette alle aziende di esercitare una metodologia di prevenzione efficace per rilevare le minacce e affrontare gli attacchi in tempo reale. Questo significa disporre di un contesto più completo che vada oltre l’endpoint, abbracciando anche email server, reti e workload cloud.

Le aziende si renderanno conto che i gap nelle competenze di cybersecurity e la scarsa attenzione alla sicurezza stessa continuano a rappresentare fattori determinanti anche nel 2020. I decision maker e i responsabili IT riconosceranno la necessità di possedere un quadro più ampio di quanto accade negli ambienti enterprise. Gli esperti della sicurezza come gli analisti SOC (Security Operations Center) saranno d’aiuto nel produrre una tale visione consolidata e nel correlare i risultati con l’intelligence globale sulle minacce.

CYBERSECURITY NEL 2020

INFORM

CNOITA

ONNECT

CYBERS

TIRUCE

Y2020202

DATA00

La collaborazione con gli esperti di sicurezza sarà essenziale per mitigare i rischi in tutte le aree dell'infrastruttura enterprise. Questo permetterà tanto agli sviluppatori quanto a chi è chiamato a difendere, di ottenere ulteriore visibilità e controllo sui dispositivi connessi e affrontare i punti deboli. Anche i rilevamenti in tempo reale e zero-hour saranno cruciali per poter identificare proattivamente le minacce note e ignote.

Il continuo mutamento dello scenario richiederà un mix intergenerazionale di difese connesse multistrato basate su meccanismi di sicurezza come:

- **Visibilità completa.** Fornisce una disamina ottimizzata e prioritizzata delle minacce per mezzo di tool e competenze che attenuano l'impatto e correggono i rischi
- **Prevenzione delle minacce con mitigazione efficace.** Attenua automaticamente le minacce una volta che sono state visualizzate e identificate, oltre a impiegare tecniche di controllo applicativo, web reputation, antispam, antimalware, machine learning e AI
- **Servizio gestito di rilevamento e risposta.** Fornisce competenze mirate capaci di correlare allarmi e rilevamenti per la scoperta delle minacce, l'analisi completa e la correzione immediata per mezzo di tool ottimizzati
- **Monitoraggio comportamentale.** Blocca proattivamente malware e tecniche avanzate, e rileva anomalie associate a malware nei comportamenti e nelle routine
- **Sicurezza degli endpoint.** Protegge gli utenti attraverso tecniche di sandboxing, rilevamento delle violazioni e sensori per endpoint che evitano gli attacchi e proteggono i dati
- **Rilevamento e prevenzione delle intrusioni.** Scoraggia il traffico sospetto come le comunicazioni C&C (Command-and-Control) e l'esfiltrazione di dati

Note

1. Catalin Cimpanu. (13 ottobre 2018). *ZDNet*. “Microsoft JET vulnerability still open to attacks, despite recent patch.” Ultimo accesso 8 ottobre 2019 https://www.zdnet.com/article/microsoft-jet-vulnerability-still-open-to-attacks-despite-recent-patch/.
2. Ionut Arghire. (29 marzo 2019). *Security Week*. “Cisco Improperly Patched Exploited Router Vulnerabilities.” Ultimo accesso 30 ottobre 2019 https://www.securityweek.com/cisco-improperly-patched-exploited-router-vulnerabilities.
3. Catalin Cimpanu. (9 settembre 2019). *ZDNet*. “Security researchers expose another instance of Chrome patch gapping.” Ultimo accesso 8 ottobre 2019 https://www.zdnet.com/article/security-researchers-expose-another-instance-of-chrome-patch-gapping/.
4. Vladimir Kropotov, Fyodor Yarochkin e Michael Ofiaza. (7 gennaio 2019). *Trend Micro Security News*. “Your Word is Your Bond: Trust and Ethics in Underground Forums.” Ultimo accesso 8 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/your-word-is-your-bond-trust-and-ethics-in-underground-forums.
5. Europol. (9 ottobre 2019). *Europol*. “Cybercrime Is Becoming Bolder With Data At The Centre Of The Crime Scene.” Ultimo accesso 11 ottobre 2019 https://www.europol.europa.eu/newsroom/news/cybercrime-becoming-bolder-data-centre-of-crime-scene.
6. Apple. (1 ottobre 2019). *Apple*. “Apple Pay participating banks in Europe and the Middle East.” Ultimo accesso 8 ottobre 2019 https://support.apple.com/en-gb/HT206637.
7. PwC. (n.d.). *PwC Italia*. “Open Banking… so what?” Ultimo accesso 28 ottobre 2019 https://www.pwc.com/it/en/industries/banking/future-open-banking.html.
8. Feike Hacquebord, Robert McArdle, Fernando Mercês e David Sancho. (17 settembre 2019). *Trend Micro Security News*. “The Risks of Open Banking.” Ultimo accesso 8 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-risks-of-open-banking-are-banks-and-their-customers-ready-for-psd2.
9. Numaan Huq, Vladimir Kropotov, Mayra Rosario, David Sancho e Fyodor Yarochkin. (28 giugno 2019). *Trend Micro Security News*. “Crimeware for Sale: The Commoditization of ATM Malware in the Cybercriminal Underground.” Ultimo accesso 8 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/crimeware-for-sale-the-commoditization-of-atm-malware-in-the-cybercriminal-underground.
10. Europol. (2018). *Europol*. “Internet Organised Crime Threat Assessment 2018.” Ultimo accesso 16 ottobre 2019 https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf.
11. The United States Department of Justice. (10 settembre 2019). *US Department of Justice*. “281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes.” Ultimo accesso 16 ottobre 2019 https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds.
12. J.M. Porup. (10 aprile 2019). *CSO Online*. “How and why deepfake videos work — and what is at risk.” Ultimo accesso 11 ottobre 2019 https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html.
13. Catherine Stupp. (30 agosto 2019). *The Wall Street Journal*. “Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case.” Ultimo accesso 11 ottobre 2019 https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.
14. Liam Tung. (4 settembre 2019). *ZDNet*. “Forget email: Scammers use CEO voice ‘deepfakes’ to con workers into wiring cash.” Ultimo accesso 16 ottobre 2019 https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/.
15. Nick Dufour and Andrew Gully. (24 settembre 2019). *Google AI Blog*. “Contributing Data to Deepfake Detection Research.” Ultimo accesso 23 ottobre 2019 *https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html*.
16. Trend Micro. (n.d.). *Trend Micro*. “Business Process Compromise (BPC).” Ultimo accesso 11 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/definition/business-process-compromise.
17. Chaoying Liu and Joseph C. Chen. (16 gennaio 2019). *Trend Micro Security Intelligence Blog*. “New Magecart Attack Delivered Through Compromised Advertising Supply Chain.” Ultimo accesso 11 ottobre 2019 https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/.
18. Catalin Cimpanu. (29 agosto 2019). *ZDNet*. “Ransomware hits hundreds of dentist offices in the US.” Ultimo accesso 24 ottobre 2019 https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/.
19. Dan Goodin. (7 settembre 2019). *Ars Technica*. “Exploit for wormable BlueKeep Windows bug released into the wild.” Ultimo accesso 24 ottobre 2019 https://arstechnica.com/information-technology/2019/09/exploit-for-wormable-bluekeep-windows-bug-released-into-the-wild/.
20. Trend Micro. (23 marzo 2018). *Trend Micro Security News*. “SAMSAM Ransomware Suspected in Atlanta Cyberattack.” Ultimo accesso 8 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/samsam-ransomware-suspected-in-atlanta-cyberattack.
21. MITRE. (19 settembre 2019). *Common Weakness Enumeration*. “CWE-502: Deserialization of Untrusted Data.” Ultimo accesso 8 ottobre 2019 https://cwe.mitre.org/data/definitions/502.html.
22. Trend Micro. (25 ottobre 2018). *Trend Micro Security News*. “Virtual Patching: Patch Those Vulnerabilities before They Can Be Exploited.” Ultimo accesso 24 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited.
23. Trend Micro. (n.d.). *Trend Micro*. “Digital Extortion.” Ultimo accesso 7 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/definition/digital-extortion.

24. Tom Wheeler and David Simpson. (3 settembre 2019). *The Brookings Institution*. "Why 5G requires new approaches to cybersecurity." Ultimo accesso 16 ottobre 2019 https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

25. Altaf Shaik and Ravishankar Borgaonkar. (2019). Black Hat. "New Vulnerabilities in 5G Networks." Ultimo accesso 16 ottobre 2019 https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf.

26. Trend Micro. (14 ottobre 2019). Trend Micro Security News. "EU Report Highlights Cybersecurity Risks in 5G Networks." Ultimo accesso 17 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/eu-report-highlights-cybersecurity-risks-in-5g-networks.

27. Tom Wheeler and David Simpson. (3 settembre 2019). *The Brookings Institution*. "Why 5G requires new approaches to cybersecurity." Ultimo accesso 6 novembre 2019 https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

28. Craig Gibson, Vladimir Kropotov, Philippe Lin, Rainer Vosselere Fyodor Yarochkin. (4 aprile 2019). *Trend Micro Security News*. "Securing Enterprises for 5G Connectivity." Ultimo accesso 16 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-enterprises-for-5g-connectivity.

29. Trend Micro. (15 agosto 2019). *Trend Micro Security News*. "Securing the Industrial Internet of Things: Protecting Energy, Water and Oil Infrastructures." Ultimo accesso 30 ottobre 2019 https://www.trendmicro.com/vinfo/ph/security/news/internet-of-things/securing-the-industrial-internet-of-things-protecting-energy-water-and-oil-infrastructures.

30. Trend Micro. (22 dicembre 2017). *Trend Micro Security News*. "TRITON Wielding Its Trident – New Malware Tampering with Industrial Safety Systems." Ultimo accesso 7 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems/.

31. Alfred Ng. (19 settembre 2019). *CNET*. "WeWork's weak Wi-Fi security leaves sensitive documents exposed." Ultimo accesso 31 ottobre 2019 https://www.cnet.com/news/weworks-weak-wi-fi-security-leaves-sensitive-documents-exposed/.

32. Trend Micro. (n.d.). *Trend Micro*. "Container." Ultimo accesso 10 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/definition/container.

33. Gartner, Inc. (4 dicembre 2018). *Gartner*. "Gartner Identifies the Top 10 Trends Impacting Infrastructure and Operations for 2019." Ultimo accesso 24 ottobre 2019 https://www.gartner.com/en/newsroom/press-releases/2018-12-04-gartner-identifies-the-top-10-trends-impacting-infras.

34. Scott Fulton III. (9 aprile 2019). *ZDNet*. "What serverless computing really means, and everything else you need to know." Ultimo accesso 24 ottobre 2019 https://www.zdnet.com/article/what-serverless-computing-really-means-and-everything-else-you-need-to-know/.

35. Guy Podjarny. (15 maggio 2018). *The Register*. "Hey cool, you went serverless. Now you just have to worry about all those stale functions." Ultimo accesso 10 ottobre 2019 https://www.theregister.co.uk/2018/05/15/stale_serverless_functions/.

36. Trend Micro. (13 aprile 2018). *Trend Micro Security News*. "Serverless Applications: What They Mean in DevOps." Ultimo accesso 10 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/serverless-applications-what-they-mean-in-devops.

37. Willem Sundblad. (18 luglio 2019). *Forbes*. "Smart Manufacturing: Creating a Hybrid Cloud-Edge Strategy." Ultimo accesso 10 ottobre 2019 https://www.forbes.com/sites/willemsundbladeurope/2019/07/18/smart-manufacturing-creating-a-hybrid-cloud-edge-strategy/#77fc5816af5a.

38. Trend Micro. (29 novembre 2018). *Trend Micro Security News*. "Hacker Infects Node.js Package to Steal from Bitcoin Wallets." Ultimo accesso 10 ottobre 2019 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets.

39. Erika Mendoza, Jay Yaneza, Gilbert Sison, Anjali Patil, Julie Cabuhate Joelson Soares. (29 marzo 2019). *Trend Micro Security Intelligence Blog*. "Emotet-Distributed Ransomware Loader for Nozelesn Found via Managed Detection and Response." Ultimo accesso 8 ottobre 2019 https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-distributed-ransomware-loader-for-nozelesn-found-via-managed-detection-and-response/.

40. Mark Vicente, Byron Galera e Augusto Remillano II. (3 aprile 2019). *Trend Micro Security Intelligence Blog*. "Bashlite IoT Malware Updated with Mining and Backdoor Commands, Targets WeMo Devices." Ultimo accesso 8 ottobre 2019 https://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-iot-malware-updated-with-mining-and-backdoor-commands-targets-wemo-devices/.

41. Steven Vaughan-Nichols. (1 luglio 2019). *ZDNet*. "Microsoft developer reveals Linux is now more used on Azure than Windows Server." Ultimo accesso 30 ottobre 2019 https://www.zdnet.com/article/microsoft-developer-reveals-linux-is-now-more-used-on-azure-than-windows-server.

42. The MITRE Corporation. (n.d.). *MITRE "ATT&CK."* Ultimo accesso 11 ottobre 2019 https://attack.mitre.org/.

Per Raimund Genes (1963-2017)

TREND MICRO™ | research

Previsioni Trend Micro sulla sicurezza per il 2020

TREND MICRO™ RESEARCH

Trend Micro, leader globale di cybersecurity, aiuta a rendere il mondo un posto sicuro per lo scambio delle informazioni digitali. Le nostre soluzioni innovative offrono ai clienti una sicurezza multi livello per i data center, i carichi di lavoro cloud, le reti e gli endpoint.

Al centro della nostra leadership, Trend Micro Research è costituita da esperti appassionati di nuove minacce, che condividono i propri insight con il pubblico per fermare i cyber criminali. Il nostro team globale aiuta a identificare milioni di minacce al giorno, è leader nella scoperta delle vulnerabilità e pubblica ricerche innovative sugli attacchi mirati, l'intelligenza artificiale, l'Internet Of Things (IoT), il mondo cyber criminale e altro ancora. Continuiamo a lavorare per anticipare la prossima ondata di minacce e per fornire ricerche che possono aiutare tutto il settore a prendere la direzione corretta.

www.trendmicro.com