TREND MICRO™ | research

# MAPPARE IL FUTURO

## Affrontare minacce pervasive e persistenti

PREVISIONI DI TREND MICRO SULLA SICUREZZA PER IL 2019

# CONTENTI




Pubblicato da Trend Micro Research

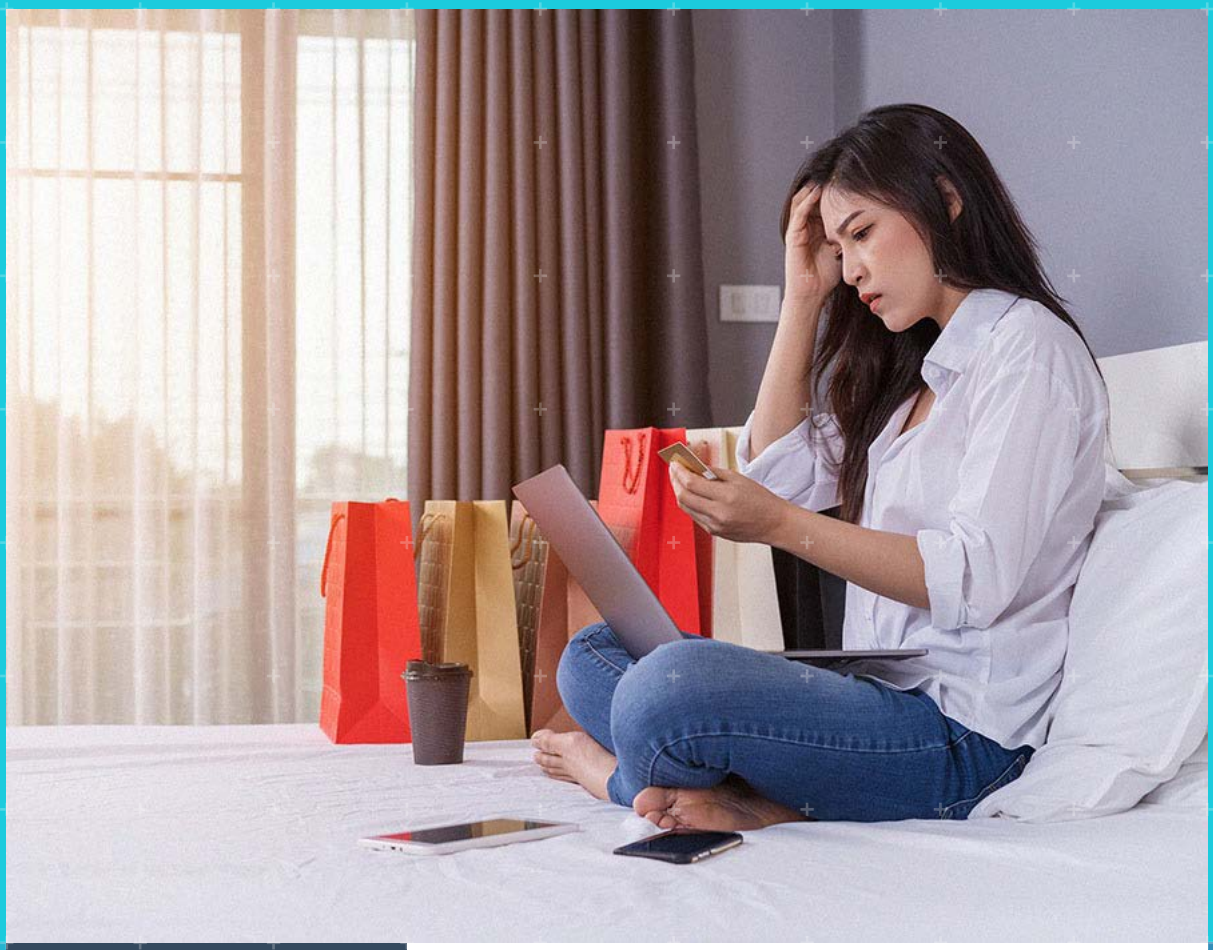
Immagini di archivio da Shutterstock.com utilizzate su licenza

# PREVISIONI DI TREND MICRO SULLA SICUREZZA PER IL 2019

Nel 2019 e non solo, le principali tendenze che si pensa avranno un impatto sulla tecnologia e la sicurezza sono i progressi nell'intelligenza artificiale e nel machine learning generati da un volume di dati elaborabili e analizzabili in continua espansione; la continua adozione del cloud computing da parte delle imprese di tutto il mondo e gli sviluppi nei settori di dispositivi, abitazioni e fabbriche intelligenti, per non parlare dell'imminente lancio del 5G nel 2020, l'ultima frontiera della comunicazione mobile, orientata verso velocità di internet sempre maggiori. Inoltre, il 2019 sarà un anno importante per gli sviluppi politici, tra cui la finalizzazione della Brexit e importanti elezioni in diversi Paesi. Questi cambiamenti tecnologici e sociopolitici avranno un impatto diretto sui problemi relativi alla sicurezza nel 2019.

Si prevede che i cyber criminali, come sempre, sfrutteranno le occasioni in cui le opportunità di profitto sono probabili, veloci e relativamente facili. Nel 2019, le implicazioni delle intrusioni digitali saranno maggiori in termini di portata e conseguenze: cresceranno i casi di frode tramite il furto di credenziali, aumenteranno le vittime di estorsioni a sfondo sessuale, si osserveranno i danni collaterali dovuti alla crescita della presenza informatica dei vari Paesi. Inoltre, il successo della cyber propaganda e delle fake news avrà il potere di decidere il destino delle nazioni. Di conseguenza, le nuove sfide per le imprese saranno dovute alla mancanza di risorse umane qualificate, che metterà sotto pressione i bilanci per la ricerca di personale IT esperto. Cresceranno le consulenze esterne. Inoltre, le cyber assicurazioni vedranno una crescita senza precedenti, in quanto si prevede un aumento anche di violazioni e mancata conformità.

Le previsioni sulla sicurezza per l'anno a venire si basano sull'analisi condotta dai nostri esperti sul progresso delle tecnologie attuali ed emergenti, sul comportamento degli utenti e sulle tendenze del mercato, nonché sull'impatto di tutto ciò sul panorama delle minacce. Abbiamo classificato queste ultime in base alle principali aree che potrebbero essere interessate, data la natura tentacolare dei cambiamenti tecnologici e sociopolitici presi in considerazione.



# CONSUMATORI

04

## Gli Exploit Kit saranno sostituiti da attacchi phishing che sfruttano tecniche di ingegneria sociale

**I casi di phishing aumenteranno sensibilmente nel 2019.** Gli attacchi di phishing, dove un aggressore finge di essere una persona o un ente con una buona reputazione in modo da indurre la vittima a rivelare dati sensibili, esistono da molto tempo. Tuttavia, nel corso degli anni, i malintenzionati hanno elaborato strategie per ridurre al minimo l'interazione con l'utente nel commettere il cyber crimine. Gli exploit kit, ad esempio, sono diventati popolari in quanto possono determinare automaticamente l'exploit da sfruttare su un obiettivo in base alle versioni di software della vittima.

Negli ultimi anni, tuttavia, una situazione di quasi-uniformità (dispositivi tutti più o meno con gli stessi software e sistemi operativi in esecuzione) sta scomparendo. Se cinque anni fa Windows era il dominatore assoluto,[1] oggi nessun singolo sistema operativo (OS) detiene più della metà del mercato.[2] I cyber criminali devono fare una scelta: passare ore su exploit o campagne che funzionano solo su una piccola porzione della popolazione di computer, contenibili con una patch dei produttori di software, oppure tornare alla tecnica classica per cui non è mai esistita una soluzione affidabile e duratura: l'ingegneria sociale.

Continueremo a osservare una diminuzione dell'attività degli exploit kit, un fenomeno che è emerso dai dati a nostra disposizione sulle attività legate a questo tipo di minaccia.

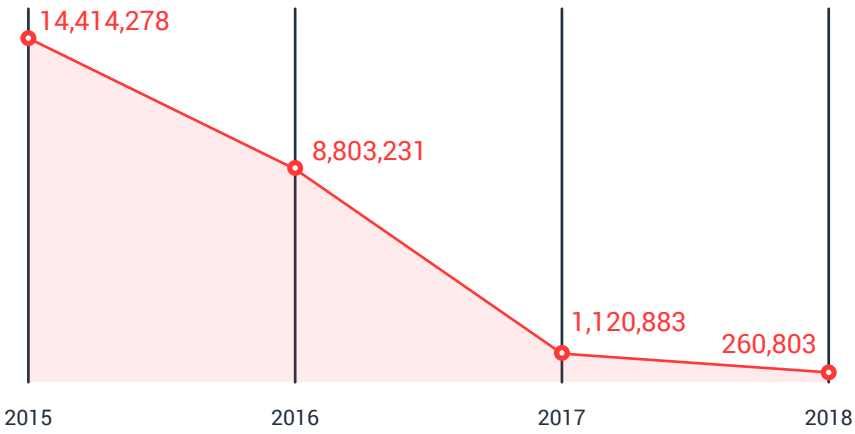



Figura 1. Le attività legate agli exploit kit sono diminuite nel corso degli anni, sulla base dei dati dell'infrastruttura Trend Micro™ Smart Protection Network™ aggiornati al Q3 2018.

Secondo i nostri feed di dati, gli attacchi di phishing stanno riprendendo e questa tendenza in crescita continuerà nel 2019.

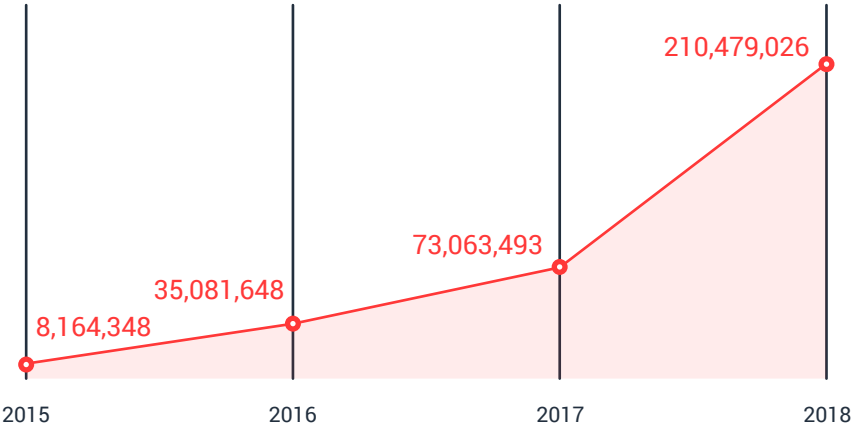



Figura 2. Il numero di URL bloccati correlati agli attacchi di phishing è cresciuto, sulla base dei dati dell'infrastruttura Trend Micro Smart Protection Network aggiornati al Q3 2018.

**Assisteremo a tentativi di phishing non solo nelle email, ma anche negli SMS e negli account di messaggistica. I cyber criminali punteranno alle solite credenziali bancarie online, ma attaccheranno anche gli account usati per l'archiviazione e altri servizi cloud. Vedremo anche dei tipi di attacco completamente nuovi, come il SIM jacking, fortemente basato sull'ingegneria sociale.** Nel SIM jacking, i criminali assumono l'identità della vittima e convincono il personale di assistenza del suo operatore telefonico a trasferire una scheda SIM "persa" in un'altra che possiedono già, assumendo di fatto il controllo della presenza online della vittima, spesso associata al numero di telefono cellulare.[3]

**In termini di contenuti di ingegneria sociale, prevediamo che i cyber criminali useranno eventi sportivi o politici nel mondo reale** come la Coppa del Mondo di rugby in Giappone nel 2019, le Olimpiadi di Tokyo nel 2020 e le imminenti elezioni in diversi Paesi. I cyber criminali, ad esempio, creeranno siti internet falsi con l'obiettivo di vendere biglietti per eventi in anticipo, sfruttare falsi annunci pubblicitari per articoli gratuiti o scontati, o inviare contenuti relativi alle elezioni o agli eventi sportivi con collegamenti dannosi.

## Ci sarà un abuso dei chat bot

La comunicazione online si è evoluta oltre la posta elettronica. Con l'uso di internet da parte di giovani più esperti e sempre online, le app di messaggistica sono ormai un canale socialmente accettato tra individui o tra un individuo e un'azienda che fornisce una forma di servizio o assistenza online al cliente. Questo nuovo formato, unito alla preferenza per l'ingegneria sociale menzionata in precedenza, aprirà a nuove opportunità per i cyber criminali.

**Prevediamo che gli attacchi che si basano sull'abuso dei chat bot dilagheranno nel 2019.** Nello stesso modo in cui gli attacchi telefonici si sono evoluti per sfruttare i messaggi preregistrati e i sistemi IVR (Interactive Voice Response), gli aggressori elaboreranno chat bot in grado di sostenere un principio di conversazione con la vittima, al fine di creare un pretesto convincente per inviare un attacco di phishing sotto forma di collegamento e ottenere informazioni personali. Gli aggressori esploreranno un'ampia gamma di possibili payload, tra cui la manipolazione di ordini, l'installazione di trojan ad accesso remoto (Remote Access Trojan, RAT) nel computer della vittima, o addirittura l'estorsione.

## Gli account delle celebrità di internet subiranno attacchi di tipo "watering hole"

Sempre in linea con la tendenza verso tecniche di ingegneria sociale più raffinate, **i cyber criminali comprometteranno gli account dei social media di famosi youtuber e altre personalità popolari online.** I cyber criminali andranno in cerca di account con diversi milioni di follower e si metteranno all'opera per impossessarsene tramite attacchi mirati di phishing e azioni simili. Tali attacchi faranno luce sulla sicurezza degli account sui principali mezzi di comunicazione, ma non prima che milioni di utenti follower di questi account siano colpiti da qualunque payload gli aggressori abbiano in serbo per loro. I computer dei follower possono essere infettati da ladri di informazioni o indotti a unirsi a campagne di denial of service distribuito (DDoS) o mining di criptovalute. I loro account possono anche essere trasformati in account troll.

## Si assisterà a un uso massiccio, nel mondo reale, di credenziali ottenute tramite violazioni dei sistemi informatici

Un recente report pubblicato da Ponemon Institute e Akamai ha messo in evidenza che il fenomeno del credential stuffing, ossia l'invio automatico di combinazioni di nome utente e password sottratte da una singola violazione a molteplici altri siti web dal diffuso utilizzo, sta diventando sempre più grave.[4] A causa del volume di violazioni di dati negli anni passati, oltre alla possibilità che i cyber criminali trovino molti utenti che riciclano le password in molti siti web, crediamo che **vedremo un aumento nelle transazioni fraudolente da parte dei cyber criminali usando credenziali ottenute tramite violazioni di dati.**

I cyber criminali useranno le credenziali rubate per ottenere vantaggi nel mondo reale, come l'iscrizione a programmi di accumulo di miglia e raccolta premi per sottrarne i benefici. I cyber criminali useranno questi account anche per registrare troll sui social media a fini di cyber propaganda, per manipolare i portali dedicati ai consumatori pubblicando false recensioni o per aggiungere voti falsi ai sondaggi rivolti alle community: le possibilità sono infinite.

## I casi di estorsione a sfondo sessuale aumenteranno

**Registreremo un incremento delle segnalazioni di adolescenti e giovani adulti vittime di estorsioni per motivi non legati al denaro, come ad esempio l'estorsione a sfondo sessuale.** Anche se non vi è alcuna garanzia che un ricattatore porterà a compimento la sua minaccia, la natura estremamente personale di questo tipo di attacchi farà sì che la vittima prenda seriamente in considerazione la possibilità di cedere alle richieste degli aggressori, che si tratti di denaro o di favori sessuali. **Con la diffusione delle estorsioni a sfondo sessuale, in particolare,[5,6,7] questo tipo di attacchi colpirà e forse creerà più vittime nel 2019.**

# AZIENDE

## Le reti domestiche utilizzate per il lavoro da remoto faranno crescere i rischi di subire un attacco alla sicurezza simili a quelli affrontati con la pratica del BYOD

**Il settore IT delle aziende vedrà sempre più attacchi dove i punti di accesso sono i dispositivi domestici dei dipendenti connessi a internet.** Si tratta dell'incrocio inaspettato ma inevitabile di due tendenze: la diffusione degli accordi di lavoro in remoto e l'adozione di dispositivi smart in ambito domestico.

Sono sempre di più i dipendenti che sfruttano la possibilità di lavorare in casa (detto anche telelavoro, lavoro mobile o lavoro da casa). Come riportato da Gallup, il 43 percento dei dipendenti statunitensi ha lavorato in remoto nel 2016, rispetto al 39 percento del 2012.[8] Secondo un sondaggio globale sulla forza lavoro condotto da Polycom, inoltre, quasi due terzi dei dipendenti hanno sfruttato il concetto di "anywhere working" nel 2017, contro appena il 14 percento nel 2012.[9] Come la filosofia del BYOD ("bring your own device", porta il tuo dispositivo), il lavoro da casa mette alla prova la visibilità dei movimenti dei dati aziendali, ogni volta che i dipendenti usano la loro connessione internet domestica per accedere ad app basate sul cloud e a software di collaborazione per chat, videoconferenze e condivisione di file.

Le reti domestiche, ormai, hanno in genere stampanti e accedono a dispositivi di archiviazione che i dipendenti trovano comodi per questioni tanto lavorative quanto personali, portando a uno scenario di utilizzo misto (ovvero, personale e aziendale). Inoltre, sono sempre di più i dispositivi domestici smart che condividono la rete domestica del lavoratore in remoto. IDC prevede una crescita a doppia cifra per tutte le categorie di dispositivi domestici smart entro il 2022.[10] Purtroppo, in termini di sicurezza, questo significa che tutti i dispositivi non protetti in una rete *domestica* di un dipendente costituiranno per gli aggressori un potenziale punto di accesso alla rete *aziendale*.

I nostri ricercatori hanno già dimostrato come gli speaker intelligenti, ad esempio, possano permettere la divulgazione di dati personali.[11] **Nel 2019, assisteremo ad alcuni scenari di attacchi mirati che faranno uso dei punti di debolezza degli speaker intelligenti per accedere alle reti aziendali attraverso le reti domestiche dei dipendenti.**

## Gli organi preposti al controllo del GDPR sanzioneranno del 4% il primo trasgressore di alto profilo

**Gli organi preposti al controllo del Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea (UE) non hanno esercitato da subito i loro nuovi poteri. Tuttavia, molto preso mostreranno un esempio di azienda non conforme, applicando l'intera sanzione del 4 percento del suo fatturato annuale globale.**

Il GDPR è un modello più maturo di rispetto della privacy. Molte organizzazioni, infatti, hanno già pagato sanzioni secondo la precedente Direttiva per la protezione dei dati per oltre un decennio, per cui i trasgressori sentiranno la morsa del regolamento prima di quanto pensino. Nel 2019, inoltre, come conseguenza del GDPR saranno rivelate più violazioni di dati rispetto all'anno passato,[12] è già stato segnalato che alcune agenzie sono inondate di nuove richieste di indagini.[13] Se si guarda il lato positivo, queste rivelazioni daranno alle aziende una maggiore visibilità e informazioni più approfondite su come i malintenzionati mettono in pericolo altre organizzazioni.

Questo porterà inevitabilmente a enfatizzare la diffusa difficoltà nel rispettare i punti più delicati del regolamento, spingendo gli organi di controllo a chiarire o aggiungere ulteriori dettagli riguardo alle tecnologie di sicurezza necessarie. **Le aziende saranno inoltre obbligate a rivalutare il valore delle attività di data mining inerenti agli attuali modelli pubblicitari, dato il caro prezzo di una possibile violazione. Infatti, prevediamo che, entro il 2020, fino al 75 percento delle nuove applicazioni aziendali dovrà sottostare a regole di conformità e sicurezza.** Per quanto la privacy e la sicurezza non si escludano a vicenda, gli sforzi per assicurare il rispetto della privacy dei dati avrà un effetto dannoso sulla capacità di un'azienda di determinare in modo adeguato l'origine e i dettagli di una minaccia per la sicurezza.

## Gli eventi nel mondo reale saranno usati per attacchi di ingegneria sociale

Nella sezione precedente, prevedevamo una maggiore diffusione degli attacchi di phishing. Nel contesto dell'impresa, **gli eventi nel mondo reale, come le imminenti elezioni in diversi Paesi nel 2019, eventi sportivi come le Olimpiadi di Tokyo nel 2020, ma anche l'instabilità politica e questioni controverse come la Brexit, costituiranno presupposti per attacchi di ingegneria sociale contro le aziende**. Prevediamo molte attività cyber criminali che sfrutteranno questi eventi e situazioni. Questi saranno usati in tipici cyber crimini, email fraudolente e ingegneria sociale contro le imprese.

I cyber criminali, inoltre, si concentreranno maggiormente sull'ottenimento di informazioni relative ai dipendenti tramite la loro presenza sui social media, in modo da architettare attacchi di phishing sempre più convincenti.

## Il Business Email Compromise scenderà di 2 livelli nell'organigramma

Il Business Email Compromise (BEC) rimane un mezzo molto potente e lucrativo per prelevare denaro dalle aziende. Crediamo che, dopo vari articoli di informazione dedicati al BEC concentrati su dirigenti vittime di frode,[14] **i cyber criminali attaccheranno dipendenti ai livelli più bassi della gerarchia aziendale.** I malintenzionati, ad esempio, punteranno alla segreteria, agli assistenti dei dirigenti, oppure ai direttori o manager nelle divisioni finanziarie.

## L'automazione sarà un nuovo problema per il Business Process Compromise

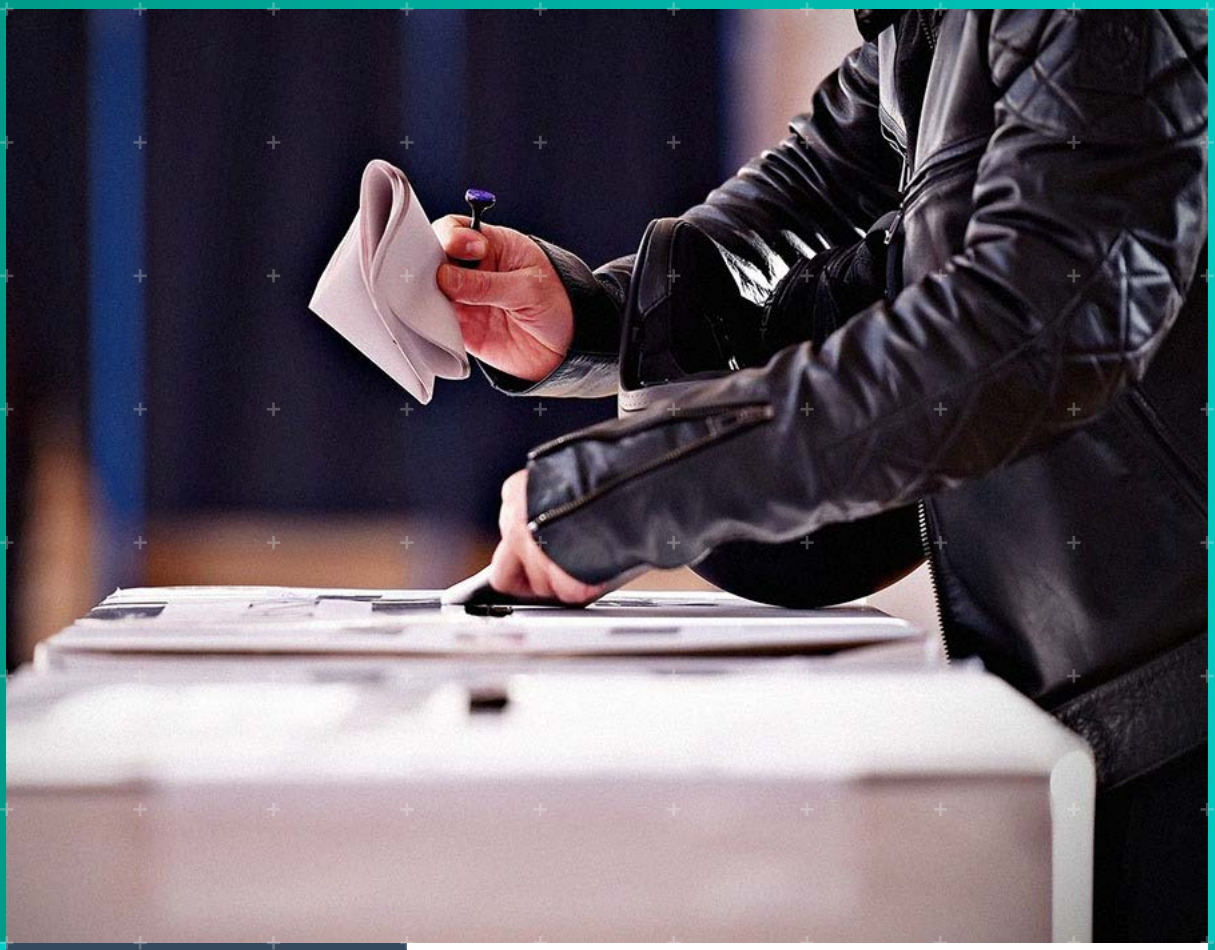
Gli attacchi di tipo Business Process Compromise (BPC), in cui specifici processi aziendali vengono impercettibilmente modificati al fine di generare profitti per gli aggressori, costituiranno un rischio costante per le imprese. **L'automazione aggiungerà un nuovo livello di sfida nella protezione dei processi aziendali contro gli attacchi di tipo BPC.** Forrester prevede che l'automazione comporterà la perdita del 10% dei posti di lavoro nel 2019.[15]

Man mano che un maggior numero di aspetti legati al monitoraggio e al funzionamento sarà trattato tramite software o applicazioni online, gli attori delle minacce avranno maggiori opportunità di infiltrarsi all'interno dei processi se questi non sono resi sicuri fin dall'inizio. Il software di automazione presenterà delle vulnerabilità e l'integrazione con i sistemi esistenti introdurrà dei varchi. Inoltre, poiché per raggiungere i propri scopi gli attori delle minacce cercheranno di scoprire i punti deboli dei fornitori e dei partner di un'azienda obiettivo, l'automazione introdurrà dei rischi anche nella filiera.

## Si esplorerà il vasto campo di applicazione dell'estorsione digitale

Date le informazioni dettagliate della nostra ricerca sul futuro del ricatto online, o estorsione digitale,[16] ci aspettiamo di vedere attuazioni o iterazioni dello stesso modello aziendale cyber criminale. Nel 2019, **vedremo i cyber criminali usare la sanzione massima per la non conformità al GDPR come linea guida o tetto massimo per la richiesta di riscatto.** Questo nella speranza che le imprese, prese dal panico e inconsapevolmente, preferiscano pagare il riscatto piuttosto che rendere nota la violazione.

Assisteremo anche ad alcuni casi di una versione di estorsione nel contesto aziendale sotto forma di campagne diffamatorie online contro i marchi. In questi casi, gli aggressori richiederanno un riscatto per smettere di diffondere propaganda in stile "fake news" contro i marchi obiettivo.



# AMMINISTRAZIONI PUBBLICHE

## La lotta contro le fake news cederà sotto la pressione di molteplici appuntamenti elettorali

Nell'UE, si prevede un "profondo cambiamento" nelle importanti elezioni per il Parlamento europeo del 2019, secondo Carnegie Europe,[17] anche perché in Paesi europei come Grecia, Polonia e Ucraina avranno luogo le rispettive elezioni politiche nazionali. Si terranno elezioni anche in Nigeria e Sudafrica, oltre a diversi Paesi in Asia, come India e Indonesia. **Crediamo che, nel 2019, i miglioramenti che i social media hanno messo in campo per combattere le fake news dopo il 2016 non saranno sufficienti per tenere il passo con il diluvio di cyber propaganda intorno a questi esercizi di democrazia.**

Come si nota nel nostro paper "La macchina delle fake news: come i propagandisti fanno abuso di internet per manipolare il pubblico", la triade necessaria per la proliferazione delle fake news può essere sconfitta solo attraverso lo smantellamento o la gestione inadeguata di uno dei suoi elementi: piattaforme, motivazione, strumenti.[18] La motivazione non mancherà mai, mentre gli strumenti sono difficili da fermare in quanto gli stessi possono essere usati per scopi legittimi. I governi hanno espresso interesse nella regolamentazione delle piattaforme di social media,[19] ma crediamo non ci sarà abbastanza tempo per questi siti per ripulire internet dalle "trasmissioni" di fake news. Nella limitazione della diffusione delle fake news, alle difficoltà tecniche si aggiunge l'utilizzo di lingue diverse nelle ampie aree geografiche come l'UE, al contrario degli Stati Uniti, dove l'inglese è la lingua più usata nei post sui social media.

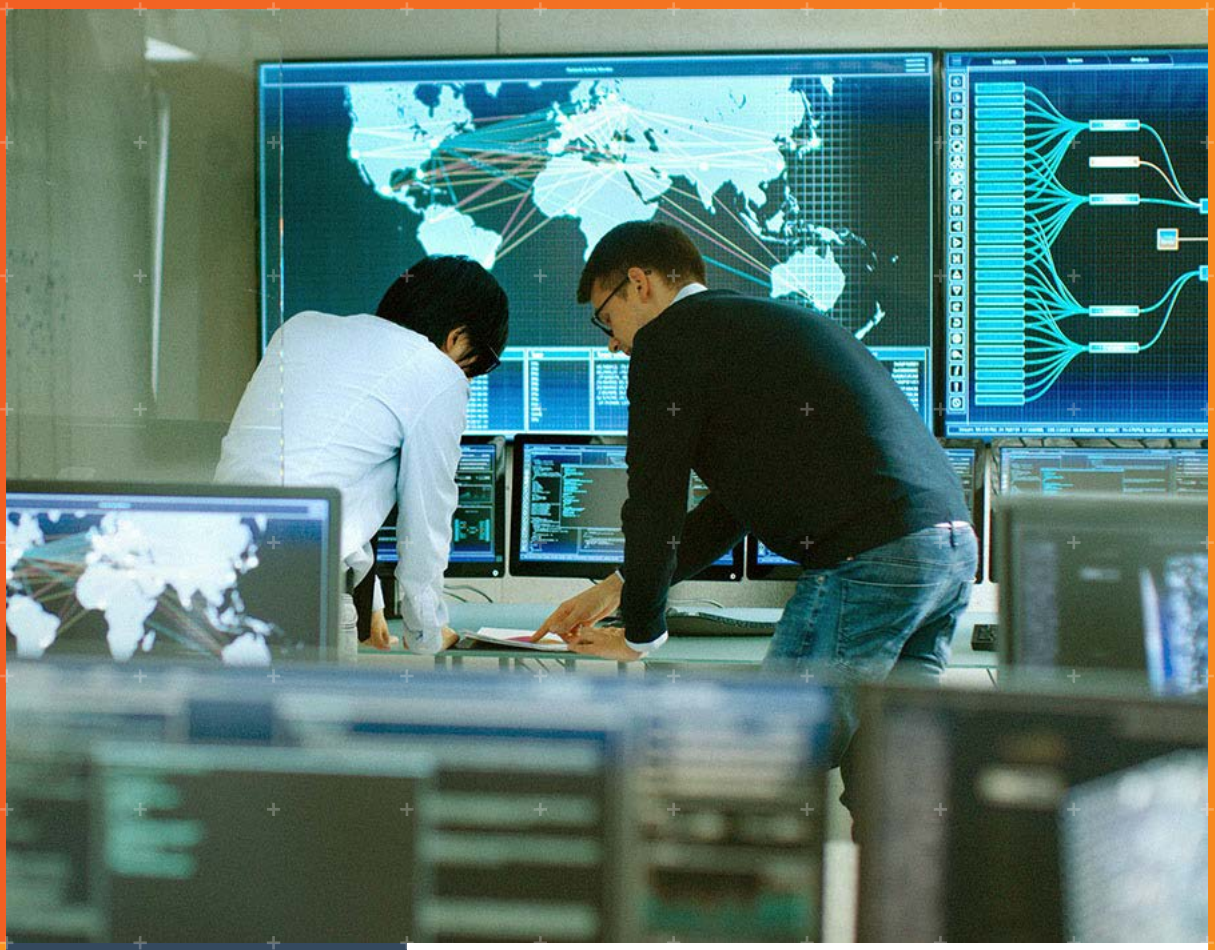
Purtroppo, le tecnologie che permettono ai propagatori di fake news di influenzare l'opinione pubblica sono ancora più potenti. Un esempio è il cosiddetto "Photoshop dell'audio" di Adobe,[20] il quale può essere benissimo sfruttato come strumento di inganno. Mentre Adobe non ha ancora diffuso nessuna ulteriore informazione relativa al software, è comunque un presagio di come si sta evolvendo la tecnologia in termini di difficoltà nel distinguere la realtà dalla finzione.

## Alcune vittime innocenti si troveranno sotto il fuoco incrociato durante il tentativo dei Paesi di espandere la propria presenza cibernetica

Continueranno a verificarsi attacchi mirati tra i protagonisti tradizionali ma, nel 2019, saranno chiamate in causa anche nazioni generalmente non coinvolte. Le nazioni che stanno rafforzando le proprie capacità informatiche, qualunque sia la ragione, cercheranno di sostenere e potenziare gli hacker nazionali, sia in ottica di difesa che di reazione ad attacchi percepiti o precedenti. **La brutta notizia è che questi sviluppi avranno effetti che ricadranno su vittime innocenti completamente estranee a queste attività di contrasto in campo informatico.** Individui e aziende, ma anche grandi organizzazioni, tra cui quelle che hanno vasti effetti sul grande pubblico, si troveranno sotto il fuoco incrociato di Paesi in lotta su come conducono le loro operazioni. Lo abbiamo già visto succedere con WannaCry[21] e NotPetya:[22] i danni collaterali potranno solo aumentare.

## Si intensificherà la vigilanza regolamentare

**Il dibattito esistente relativo alla sicurezza spingerà le amministrazioni pubbliche a intensificare la vigilanza regolamentare non solo in materia di privacy, ma anche nei segmenti industriali e relativi al consumatore dell'Internet delle cose (IoT).** Negli Stati Uniti, la legge della California che obbliga i produttori a usare password sicure nei loro dispositivi smart è solo un passo in questa direzione.[23] Ci aspettiamo di vedere i governi nazionali proibire l'uso di IoT device industriali e diretti al consumatore, non sicuri a partire da leggi che verranno introdotte nel 2019.



# SETTORE DELLA SICUREZZA

## I cyber criminali utilizzeranno un maggior numero di tecniche per mimetizzarsi

In risposta alle tecnologie dei fornitori di sicurezza, in particolare al rinnovato interesse per l'applicazione del machine learning alla cybersecurity, **i cyber criminali utilizzeranno tattiche più subdole per "mimetizzarsi".** Si continueranno a scoprire, documentare e condividere nuovi modi di utilizzare normali oggetti informatici per usi o scopi diversi da quelli previsti, una pratica nota come "Vivere fuori dagli schemi". Abbiamo osservato diversi casi di questo tipo, tra cui:

- L'uso di estensioni di file non convenzionali come .URL, .IQY, .PUB, .ISO e .WIZ.
- Minore affidamento su effettivi file eseguibili, come nel caso dell'uso di componenti "fileless", Powershell, script e macro.
- Malware con firma digitale, come già osservato nella nostra ricerca "Exploring the Long Tail of (Malicious) Software Downloads",[24] una tecnica ormai incontrollata che sarà sempre abusata per la sua efficacia.
- Nuovi metodi di attivazione, oltre a tecniche già esaminate come l'uso di Mshta, Rundll32, Regasm o Regsvr32.[25]
- L'abuso di account email o servizi di archiviazione online e app come punti di accesso di comando e controllo o come siti di download o di esfiltrazione.
- Modifiche o infezioni minimali di file di sistema legittimi.

Le imprese che si affidano alla tecnologia di machine learning come *unica* soluzione di sicurezza dovranno affrontare una grande sfida man mano che molti cyber criminali utilizzeranno queste tecniche, tra le altre, per infettare i sistemi. Ci aspettiamo che tali tattiche a uso dei cyber criminali diventino molto più diffuse nel 2019.

## Il 99,99% degli attacchi basati su exploit non sarà comunque basato sulle vulnerabilità zero-day

Gli exploit zero-day, componenti di malware in the wild che sfruttano vulnerabilità del software di cui i fornitori sono ignari, sono stati un punto centrale nel settore della sicurezza IT, facendo notizia a ogni scoperta di un nuovo attacco, in quanto relativamente rari.

Da una parte, per i cyber criminali è difficile scoprire vulnerabilità di software nuove a causa dell'infrastruttura esistente di divulgazione responsabile che premia i ricercatori di vulnerabilità per le loro scoperte, tra cui la Zero Day Initiative (ZDI) di Trend Micro. E se ci riescono, comunque, tutto ciò che serve affinché i produttori siano sollecitati a prendere le misure adeguate

è la scoperta dell'attacco. D'altro canto, l'opportunità più accessibile per i cyber criminali è la finestra di esposizione che si apre tra il rilascio di una nuova patch e quando questa viene implementata sui sistemi aziendali. Gli amministratori avranno bisogno della strategia e della quantità di tempo adatte per applicare le patch. Questi problemi di efficienza daranno ai cyber criminali il tempo sufficiente per preparare un attacco. Siccome i dettagli stessi della vulnerabilità sono stati pubblicati al momento della divulgazione, il tempo di ricerca per sfruttare la debolezza è significativamente ridotto.

**Nel 2019, gli attacchi basati sugli exploit conclusi con successo riguarderanno vulnerabilità per le quali sono disponibili patch da settimane, o addirittura da mesi, che non sono ancora state applicate.** Continueremo a vedere casi di exploit n-day come un assillo per la sicurezza della rete.

## Gli attacchi altamente mirati inizieranno a sfruttare tecniche basate sull'IA

**Gli attacchi mirati da parte di aggressori ben finanziati inizieranno a sfruttare tecniche di ricognizione basate sull'intelligenza artificiale (IA)** L'uso dell'IA darà loro la possibilità di prevedere i movimenti dei dirigenti o altre persone di interesse. Possono usare l'IA per determinare quando e dove i dirigenti aziendali potrebbero trovarsi in futuro, ad esempio gli hotel in cui risiederanno per conto dell'azienda, i ristoranti scelti per gli incontri di lavoro e altre preferenze utili a individuare la loro prossima probabile posizione.

I fornitori di sicurezza, da parte loro, escogiteranno a loro volta delle tecniche di difesa tramite IA. I team di sicurezza si affideranno a loro volta all'IA, più o meno come con il machine learning, per capire in maniera più profonda in cosa consistono le attività di base di un'azienda per essere avvisati immediatamente quando si verifica qualcosa di anormale dal punto di vista della sicurezza. Questi scenari futuristici danno uno sguardo alla prossima frontiera della tecnologia IA e cosa questo comporta per la sicurezza.


# SISTEMI PER IL CONTROLLO INDUSTRIALE

## Gli attacchi ai sistemi per il controllo industriale (Industrial Control Systems, ICS) diventeranno una preoccupazione crescente.

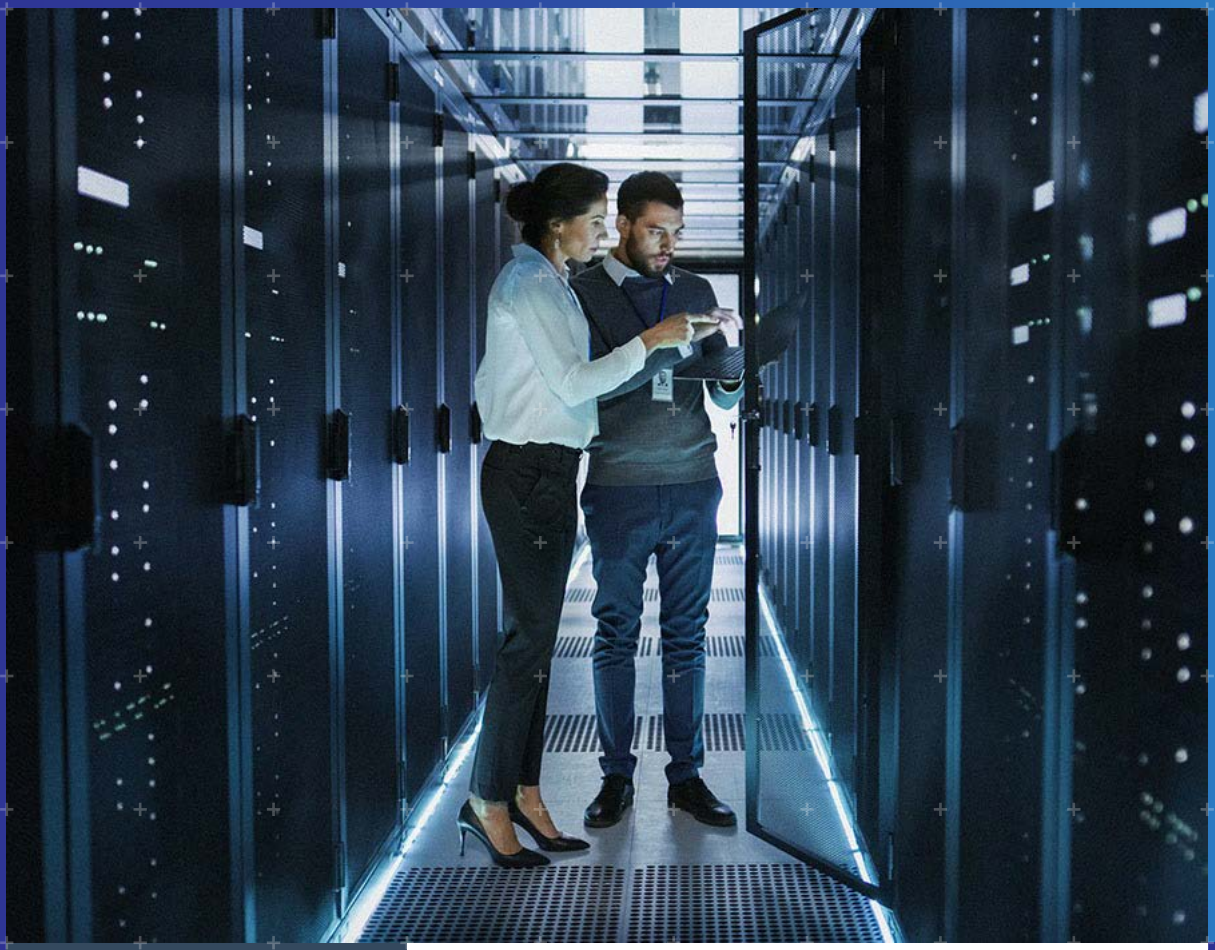
**I Paesi che stanno acquisendo ed esercitando le loro capacità informatiche condurranno attacchi contro le infrastrutture critiche dei protagonisti minori.** Tra le altre possibili motivazioni, lo faranno per ottenere un vantaggio politico o militare, o per testare le loro capacità contro Paesi che non hanno ancora la possibilità di applicare ritorsioni. La possibilità che gli attacchi si concentrino su sistemi per il controllo industriale (ICS) dedicati alla gestione delle acque, dell'elettricità o della produzione industriale, dipenderà dall'intenzione o dall'opportunità che si presenterà all'attore della minaccia. Gli incidenti, tuttavia, metteranno in evidenza le debolezze come quelle che dovrebbero essere limitate dalla direttiva sulla sicurezza delle reti e dei sistemi informatici (Direttiva NIS) con i suoi regolamenti per gli operatori di servizi essenziali.[26]

Questi attacchi si attueranno come ogni altro attacco mirato che inizia con una fase di ricognizione fino al raggiungimento degli obiettivi dell'aggressore. Un attacco ICS di successo avrà effetti sull'infrastruttura obiettivo con spegnimenti operativi, danneggiamento di apparecchiature, perdite finanziarie indirette e, nel peggiore dei casi, rischi per la salute e la sicurezza.

## I bug nella IUM saranno ancora l'origine principale delle vulnerabilità ICS

In base ai dati di ZDI, gran parte delle vulnerabilità legate al software usato con sistemi di controllo di sorveglianza e acquisizione dati (SCADA) sono state rilevate nelle interfacce uomo-macchina (IUM),[27,28] usate come centro di gestione principale dei vari moduli di diagnostica e controllo in una struttura. I sistemi ICS in generale, compresi i sistemi di controllo distribuito (DCS), nonché diversi dispositivi di campo e i sistemi SCADA, si avvalgono tutti di una forma di IUM e, **nel 2019, vedremo ancora più segnalazioni di vulnerabilità di IUM**.

Allo stato attuale, questi tipi di software sono facilmente materia di studio per i ricercatori di vulnerabilità. È ormai noto, inoltre, che il software IUM non è solido e sicuro come il software di aziende come Microsoft e Adobe per varie ragioni, tra cui la supposizione errata secondo cui questo tipo di software sarà eseguibile solo in ambienti isolati o con air gap.[29] Oltretutto, la manutenzione e l'aggiornamento del software IUM possono essere ostacolati o influenzati dai movimenti presenti sul mercato di piccoli venditori acquisiti da altri più grandi, o attori locali che si fondono con altri.



# INFRASTRUTTURE CLOUD

## Le configurazioni di sicurezza non corrette nelle migrazioni cloud, daranno origine a ulteriori violazioni di dati

La migrazione dei dati nel cloud è uno sforzo che riguarda tutta l'azienda e richiede lo stesso livello di pianificazione, impegno e coinvolgimento di un trasloco fisico, se non maggiore. Ogni migrazione nel cloud è unica in termini di portata e ritmo e la best practice di ogni settore dovrà sempre essere adeguata alle circostanze specifiche e ai bisogni reali di un'azienda.

**Prevediamo di assistere a molti più casi gravi di violazione di dati come risultato diretto di configurazioni non corrette durante la migrazione nel cloud.** La transizione dei dati da un cloud privato o locale a un fornitore di servizi cloud può esporre un'impresa a rischi di sicurezza, a meno che l'impresa non abbia piena coscienza su quanto stia accadendo ai suoi dati. I bucket di archiviazione del cloud possono essere privati per definizione, ma un bucket esterno esistente porterà con sé le sue autorizzazioni. I criteri di accesso devono quindi essere compresi, implementati e mantenuti in modo adeguato in tutte le fasi di utilizzo del bucket.

## Le istanze cloud saranno sfruttate nel mining di criptovalute

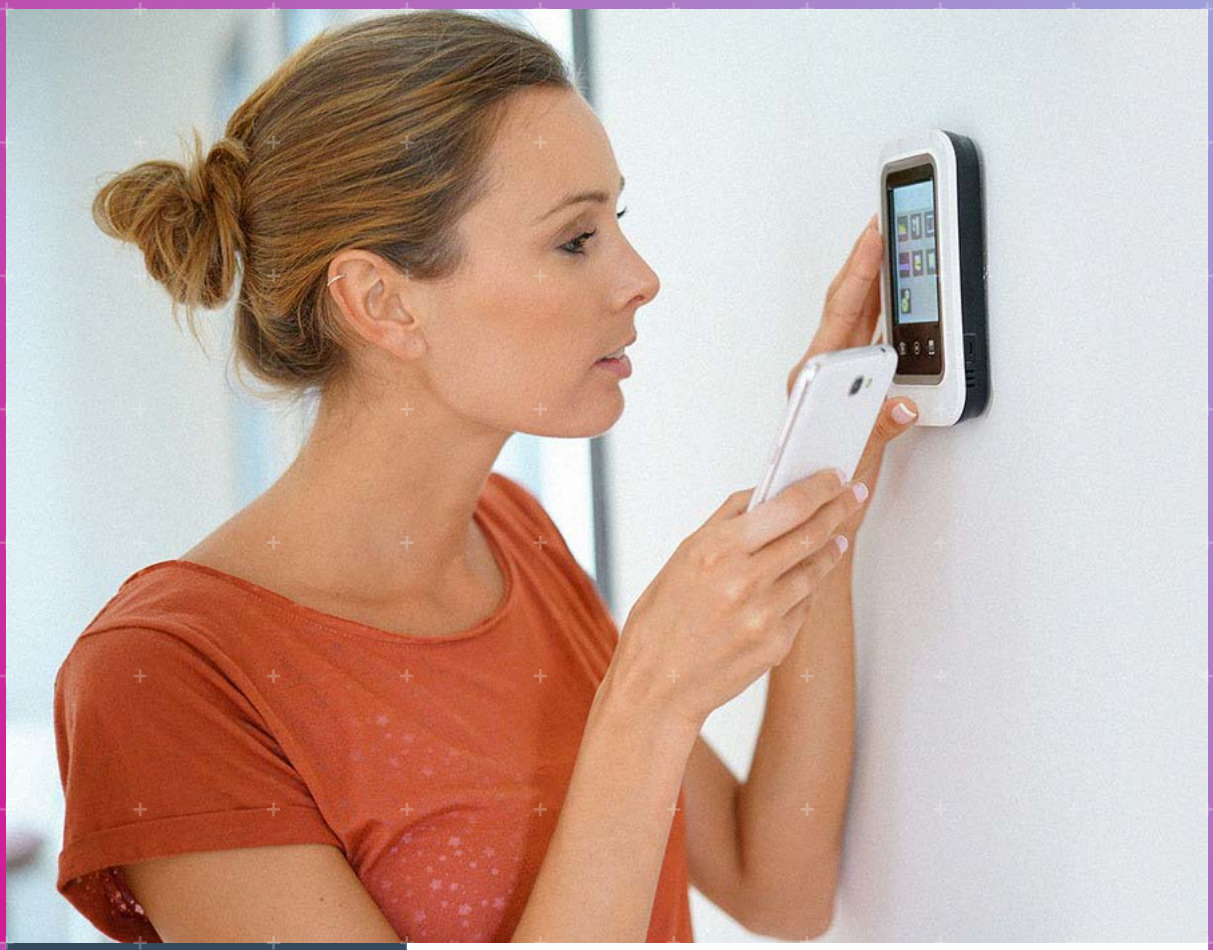
Il cloud mining è un'alternativa reale per gli onesti appassionati di mining di criptovalute in cui, in parole semplici, un miner acquista potenza della CPU da un fornitore invece di investire in apparecchiature. Esistono diversi piani di pagamento per questo modello commerciale, ma la principale attrattiva del cloud mining consiste nell'essere una pratica semplice da avviare e mantenere, rendendolo accessibile ai miner per cui l'hardware o l'elettricità possono costituire un problema.

Senza sforzare troppo l'immaginazione, **sempre più cyber criminali tenteranno di assumere il controllo degli account cloud per il mining di criptovalute o di mantenerlo sulle alternative**. Questo significa che i casi riportati dai media di cryptojacking (l'uso non autorizzato di computer per il mining di criptovalute) scoperti negli ambienti cloud nel 2018 sono un segno di una tendenza in crescita,[30] non un tentativo isolato da parte di cyber criminali. Sono già disponibili strumenti di scansione dei bucket del cloud. A questo va aggiunta la difficoltà di configurare correttamente tutte le impostazioni di sicurezza di ciascuna implementazione cloud. I cyber criminali troveranno inevitabilmente un modo per muoversi in questa direzione. Ci aspettiamo inoltre che i malware di cryptojacking riducano al minimo i rischi di rilevamento riducendo l'utilizzo delle risorse.

## Sarà scoperto e sfruttato un numero maggiore di vulnerabilità legate al cloud

In termini di preferenze dell'aggressore, i cyber criminali andranno ancora a caccia di prede semplici come le credenziali degli account per accedere agli asset del cloud e controllare i database. La ricerca nel campo delle debolezze dell'infrastruttura cloud, tuttavia, non resterà a guardare. **Con l'aumento dell'adozione del cloud, vedremo la ricerca delle vulnerabilità dell'infrastruttura cloud iniziare a intensificarsi,** soprattutto perché la comunità open source scoprirà più utilizzi e analizzerà più in profondità i software relativi al cloud come Docker, un programma di containerizzazione, o Kubernets, un sistema di orchestrazione dei container.

Sia Docker[31] che Kubernetes[32] sono ampiamente adottati per l'utilizzo in distribuzioni basate su cloud. Negli anni recenti, sono già state rilevate alcune vulnerabilità di Kubernets,[33] di cui una "critica" scoperta nel dicembre 2018.[34] Nel frattempo, in analisi approfondite delle vulnerabilità dell'infrastruttura cloud da parte dei ricercatori, Kromtech ha scoperto più di una dozzina di immagini Docker dannose, scaricate almeno cinque milioni di volte da ignari sviluppatori, nel corso di un anno prima di essere rimosse.[35]



# SMART HOME

## I cyber criminali competeranno per il predominio in una nascente "Worm War" nel campo dell'IoT

Con un numero crescente di dispositivi smart connessi alle reti domestiche, i router continueranno a essere un interessante vettore di attacco per i cyber criminali intenzionati ad assumere il controllo di qualsiasi dispositivo connesso, indipendentemente dallo scopo. **L'ambiente delle smart home vedrà ripetersi un'era tecnicamente memorabile nella storia della sicurezza informatica: le cosiddette "worm war" scoppiate all'inizio degli anni 2000**.[36]

I recenti attacchi basati su router che riguardano i dispositivi intelligenti, o gli attacchi IoT, sono per lo più basati sullo stesso codice sorgente trapelato dal malware Mirai,[37] che per primo infettò i dispositivi interconnessi su Linux nell'agosto 2016,[38] o da altri malware che si comportano in modo analogo. Questi elementi malware usano alcuni exploit conosciuti e credenziali di accesso e password prevalentemente poco sicuri per introdursi nei dispositivi. Questo significa che eseguono tutti una scansione automatica di internet scoprendo gli stessi identici dispositivi. Poiché esiste un numero finito di dispositivi e solo un malware deve avere il controllo di un singolo dispositivo per eseguire payload e svolgere attività dannose come attacchi DDoS, i cyber criminali inizieranno ad aggiungere codice per impedire a qualsiasi altro hacker di utilizzare il dispositivo o per estromettere un malware esistente, diventandone quindi i proprietari esclusivi. Gli esperti di sicurezza troveranno familiari questi comportamenti: i creatori di Netsky iniziarono una worm war contro gli hacker dietro altri due noti worm dell'epoca, Mydoom e Bagle.

## Emergeranno i primi casi di persone anziane che cadono vittime di attacchi a dispositivi sanitari intelligenti

Ricercatori, appassionati e aggressori continueranno in egual misura a scoprire nuove vulnerabilità nei dispositivi smart. Tuttavia, gli attacchi reali resteranno sporadici nei prossimi anni finché i cyber criminali non troveranno una via proficua, chiara e semplice. Oltre il 2019, è facile immaginare come i ricercatori di vulnerabilità o anche gli hacker cercheranno di inserirsi in dispositivi e sistemi smart, in particolare quelli legati a ricerche e adozioni di mercato significative, come le connected car.[39] Per il momento, i cyber criminali sono esclusivamente interessati al denaro. Siccome esistono molte altre strade proficue, un attacco globale ai dispositivi smart risulta improbabile nel 2019.

Nel contesto più ristretto dei tracker sanitari, tuttavia, crediamo che **le prime vittime reali di attacchi a dispositivi sanitari intelligenti saranno le persone anziane.** Le aziende stanno esplorando la platea di clienti anziani come potenziali utenti di smart tracker o altri dispositivi sanitari connessi a internet,[40] come quelli che monitorano la frequenza cardiaca o che emettono avvisi agli account collegati quando l'utente anziano scivola o cade. In passato, le persone anziane sono state bersaglio di truffe telefoniche a causa della loro relativa ricchezza, data dal loro risparmio previdenziale.[41] Crediamo che gli anziani diventeranno facili vittime di attacchi che abusano di questi dispositivi già nel 2019. Da un lato, gli utenti anziani di tracker sanitari non saranno abbastanza esperti di computer per controllare le impostazioni della privacy di questi dispositivi (con conseguente divulgazione di dati medici personali) o per mantenere sicuri i propri account (consentendo ai cyber criminali di accedere ai dati personali relativi alla salute e di altro tipo).

Dopo il 2019, vedremo anche più "attacchi vocali"[42] colpire utenti di tutte le età. La ricerca nelle vulnerabilità nei sistemi intelligenti di riconoscimento vocale è in crescita, mentre i dispositivi smart di assistenza sono una funzionalità sempre più diffusa nelle smart home.

# PREPARARSI PER L'ANNO IN CORSO

## Ulteriori incognite richiedono una sicurezza multistrato e intelligente per le imprese

Le realtà delle architetture dei datacenter ibridi moderni, nonché l'evoluzione dell'accesso e la mobilità tra endpoint e utente finale (tra cui partner e altre terze parti connesse alla rete) richiederanno molto di più dai team di sicurezza IT nel 2019. La carenza di competenze di sicurezza IT sarà quindi ancora più pronunciata e l'incremento delle competenze attuali con tecnologie di sicurezza intelligenti,[43] efficienti e a più livelli sarà ancora più cruciale.

Proteggere le reti aziendali dalle minacce in continua evoluzione richiede un'acuta percezione di come andrebbero gestiti i rischi relativi alla sicurezza. L'intera gamma di minacce, conosciute e sconosciute, non potrà mai essere affrontata da un'unica, moderna tecnologia, in quanto ciascuna nuova tipologia di minacce costituisce una sfida in diversi aspetti della sicurezza IT. Le aziende non dovrebbero cercare una bacchetta magica, ma piuttosto un mix intergenerazionale di tecniche di difesa dalle minacce che applica intelligentemente la giusta tecnica al momento giusto:

- Prevenzione dei malware (programmi antimalware, machine learning, analisi della web reputation).
- Sicurezza di rete (prevenzione delle intrusioni, firewall, analisi delle vulnerabilità).
- Sicurezza per email e collaborazione (antispam).
- Sicurezza del sistema (controllo delle applicazioni, monitoraggio dell'integrità, controllo del registro).
- Motori di rilevamento specializzati, sandboxing personalizzato e intelligence contro le minacce mondiali (per le minacce sconosciute).
- Sicurezza endpoint.
- Prevenzione integrata della perdita di dati.

Sarebbe opportuno adattare questa soluzione a dove e come gli utenti realmente si connettono alla rete in termini di piattaforme e dispositivi. Infine, queste tecnologie devono dare la possibilità ai team di sicurezza IT di visualizzare le attività di rete, valutare le minacce e intraprendere le misure necessarie.

## Gli sviluppatori devono abbracciare la cultura DevOps tenendo sempre a mente la sicurezza

DevOps unisce i processi di sviluppo del software (Dev) alle operazioni IT (Ops) per abbreviare il ciclo di vita di sviluppo del sistema in modo molto più efficiente e integrato. L'approccio DevSecOps, ossia DevOps con particolare attenzione alla sicurezza, porta a robuste pratiche di sicurezza e sicurezza incorporata in ogni fase del processo. Gli sviluppatori di software dovrebbero adottare questa mentalità, insieme alla sua pratica gamma di strumenti, al fine di ottenere non

solo vantaggi per la sicurezza ma anche una riduzioni dei costi. Le debolezze progettuali e altre vulnerabilità, comprese quelle che causano fughe di dati personali, sono spesso scoperte dopo l'installazione del software nei computer o dispositivi di produzione, e potrebbero diminuire sensibilmente se la sicurezza fosse integrata nello sviluppo fin dalla fase di pianificazione.

## ▶ Gli utenti devono assumere una cittadinanza digitale responsabile e applicare le best practice in tema di sicurezza

La capacità degli utenti di distinguere la realtà dalla finzione, in particolare su internet, sarà più importante nel 2019. Si spera che, con la diffusione di consapevolezza sulle meccaniche dietro alle fake news, il pubblico diventi più immune alla manipolazione dell'opinione. Le amministrazioni locali e statali faranno bene a includere programmi di formazione sulla cybersecurity nelle scuole e diffondere la conoscenza al grande pubblico.

L'ingegneria sociale, essenzialmente, si basa sulle debolezze umane, per cui gli utenti devono applicare lo stesso livello di pensiero critico necessario sui social media, così come al controllo della provenienza di un'email o di una telefonata da una fonte effettivamente attendibile.

I dispositivi dei consumatori, come computer, tablet e smartphone, devono essere protetti da minacce come ransomware, siti pericolosi e furti di identità, soprattutto assicurandosi di avere a disposizione una protezione completa tramite soluzioni di antimalware. Queste tecnologie devono anche includere la protezione dei dati per salvaguardare i file di valore, sventare nuove minacce e assicurare che le transazioni monetarie online siano eseguite in sicurezza.

Gli utenti dovrebbero cambiare le loro password regolarmente, utilizzare password univoche per diversi account, sfruttare le funzionalità di autenticazione multifattore ogni volta che è possibile oppure utilizzare uno strumento di gestione delle password per conservare le credenziali in modo sicuro.

Gli amministratori delle smart home dovrebbero anche proteggere i router e i dispositivi verificando le impostazioni predefinite dei prodotti e comprendendo come configurarle in modo sicuro, aggiornando il firmware regolarmente, connettendosi solo a reti sicure, configurando firewall per consentire il traffico solo su porte specifiche e impostando "reti ospiti" per ridurre al minimo l'introduzione non necessaria di nuovi dispositivi nella rete. Inoltre, dove possibile, i proprietari dovrebbero esaminare la cronologia dei registri dei dispositivi. Ovviamente, sarebbe opportuno applicare password univoche e sicure anche per router e dispositivi.

**Nel 2019, il panorama delle minacce promette molte sfide per gli utilizzatori di internet, in praticamente tutti i settori, anche perché, all'orizzonte, si profila l'arrivo di un internet più veloce (nel bene e nel male) con il lancio del 5G. Gli strumenti e le tecnologie disponibili, tuttavia, dovrebbero permettere a utenti e aziende di avere una posizione più sicura nella lotta contro i cyber criminali e altre minacce emergenti. Una maggiore comprensione di questi problemi costituisce un passo nella direzione giusta.**

# References


1. StatCounter. *Statcounter Global Stats.* "Operating System Market Share Worldwide, Jan-Dec 2013." Last accessed on 13 November 2018 at http://gs.statcounter.com/os-market-share/all/worldwide/2013.

2. StatCounter. *Statcounter Global Stats.* "Operating System Market Share Worldwide, Oct 2017 – Oct 2018." Last accessed on 13 November 2018 at http://gs.statcounter.com/os-market-share.

3. Lorenzo Franceschi-Bicchierai. (17 July 2018). *Motherboard.* "The SIM Hijackers." Last accessed on 13 November 2018 at https://motherboard.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin.

4. Ponemon Institute. (June 2018). *Akamai.* "The Cost of Credential Stuffing: Asia-Pacific." Last accessed on 13 November 2018 at https://www.akamai.com/us/en/multimedia/documents/white-paper/the-cost-of-credential-stuffing-asia-pacific.pdf

5. Donna Freydkin. (9 February 2018). *Today.* "How online 'sextortion' drove one young man to suicide." Last accessed on 28 November 2018 at https://www.today.com/parents/how-online-sextortion-drove-one-young-man-suicide-t122735

6. Lizzie Dearden. (4 May 2018). *Independent.* "Five British men have killed themselves after falling victim to online 'sextortion', police reveal." Last accessed on 28 November 2018 at https://www.independent.co.uk/news/uk/crime/blackmail-online-sextortion-suicides-videos-photos-sexual-police-advice-a8337016.html

7. David Goodwin. (8 November 2018). *Greenock Telegraph.* "Inverclyde youngsters fall victim to 'sextortion' gangs." Last accessed on 28 November 2018 at https://www.greenocktelegraph.co.uk/news/17204102.inverclyde-youngsters-fall-victim-to-sextortion-gangs/

8. Gallup. (2017). *Gallup.* "State of the American Workplace." Last accessed on 27 November 2018 at https://news.gallup.com/file/reports/199961/SOAW_Report_GEN_1216_WEB_FINAL_rj.pdf.

9. Polycom. (2018). *Polycom.* "The Changing World of Work." Last accessed on 13 November 2018 at http://www.polycom.com/content/dam/polycom/common/documents/whitepapers/changing-needs-of-the-workplace-whitepaper-enus.pdf

10. IDC. (1 October 2018). *IDC.* "All Categories of Smart Home Devices Forecast to Deliver Double-Digit Growth Through 2022, Says IDC." Last accessed on 13 November 2018 at https://www.idc.com/getdoc.jsp?containerId=prUS44361618.

11. Stephen Hilt. (27 December 2018). *Trend Micro Security Intelligence Blog.* "The Need for Better Built-in Security in IoT Devices." Last accessed on 13 November 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/iot-devices-need-better-builtin-security/.

12. Greg Young and William J. Malik. (3 May 2018). *Trend Micro Simply Security.* "What HIPAA and Other Compliance Teaches Us About the Reality of GDPR." Last accessed on 13 November 2018 at https://blog.trendmicro.com/what-hipaa-and-other-compliance-teaches-us-about-the-reality-of-gdpr/.

13. Phil Muncaster. (14 September 2018.) *Infosecurity Magazine.* "ICO Swamped with GDPR Breach Over-Reporting." Last accessed on 28 November 2018 at https://www.infosecurity-magazine.com/news/ico-swamped-with-gdpr-breach/.

14. David Meyer. (4 December 2018). *Fortune.* "How Email Scammers Are Using Marketeer Methods to Target CFOs." Last accessed on 5 December 2018 at http://fortune.com/2018/12/04/targeted-email-fraud/.

15. Forrester Research. (14 November 2018). *ZDNet.* "Automation will become central to business strategy and operations." Last accessed on 14 November 2018 at https://www.zdnet.com/article/automation-will-become-central-to-business-strategy-and-operations/.

16. David Sancho. (30 January 2018). *Trend Micro Security Intelligence Blog.* "Digital Extortion: A Forward-looking View." Last accessed on 13 November 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/digital-extortion-forward-looking-view/.

17. Alberto Alemanno. (27 June 2018). *Carnegie Europe.* "Europe Up for Grabs: The Looming Battle Lines of the 2019 European Parliament Elections." Last accessed on 13 November 2018 at https://carnegieeurope.eu/2018/06/27/europe-up-for-grabs-looming-battle-lines-of-2019-european-parliament-elections-pub-76691.

18. Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin. (13 June 2017). *Trend Micro Security News.* "Fake News and Cyber Propaganda: The Use and Abuse of Social Media." Last accessed on 13 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media.

19. Charles Hymas. (20 September 2018). *The Telegraph.* "Government draws up plans for social media regulator following Telegraph campaign." Last accessed on 13 November 2018 at https://www.telegraph.co.uk/news/2018/09/20/government-draws-plans-social-media-regulator-following-telegraph/.

20. Sebastian Anthony. (7 November 2018). *Ars Technica.* "Adobe demos "photoshop for audio," lets you edit speech as easily as text." Last accessed on 13 November 2018 at https://arstechnica.com/information-technology/2016/11/adobe-voco-photoshop-for-audio-speech-editing/.

21. Lily Hay Newman. (12 May 2017). *Wired.* "The Ransomware Meltdown Experts Warned About Is Here." Last accessed on 28 November 2018 at https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.

22. Andy Greenberg. (22 August 2018). *Wired.* "The Untold Story of Notpetya, The Most Devastating Cyberattack in History." Last accessed on 28 November 2018 at https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

23. Adi Robertson. (28 September 2018). *The Verge.* "California just became the first state with an Internet of Things cybersecurity law." Last accessed on 13 November 2018 at https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law.

24. Trend Micro Forward-Looking Threat Research Team. (5 April 2018). *Trend Micro Security Intelligence Blog.* "Understanding Code Signing Abuse in Malware Campaigns." Last accessed on 13 November 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/understanding-code-signing-abuse-in-malware-campaigns/.

25. MITRE ATT&CK. *MITRE.* "Tactic: Execution." Last accessed on 13 November 2018 at https://attack.mitre.org/tactics/TA0002/.

26. European Union Agency for Network and Information Security. *ENISA.* "NIS Directive." Last accessed on 5 December 2018 at https://www.enisa.europa.eu/topics/nis-directive.

27. Trend Micro. (23 May 2017). *Trend Micro Security News.* "The State of SCADA HMI Vulnerabilities." Last accessed on 13 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities.

28. Brian Gorenc. (9 July 2018). *Zero Day Initiative.* "Checking In: A Look Back at the First Half of 2018." Last accessed on 28 November 2018 at https://www.zerodayinitiative.com/blog/2018/7/9/checking-in-a-look-back-at-the-first-half-of-2018.

29. Trend Micro. (23 May 2017). *Trend Micro Security News.* "The State of SCADA HMI Vulnerabilities." Last accessed on 13 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities.

30. Charlie Osborne. (15 May 2018). *ZDNet.* "Cryptojacking attacks surge against enterprise cloud environments." Last accessed on 28 November 2018 at https://www.zdnet.com/article/cryptojacking-attacks-surge-against-enterprise-cloud-environments/.

31. Steven J. Vaughan-Nichols. (21 March 2018). *ZDNet.* "What is Docker and why is it so darn popular?" Last accessed on 28 November 2018 at https://www.zdnet.com/article/what-is-docker-and-why-is-it-so-darn-popular/.

32. Udi Nachmany. (1 November 2018). *Forbes.com.* "Kubernetes: Evolution of an IT Revolution." Last accessed on 28 November 2018 at https://www.forbes.com/sites/udinachmany/2018/11/01/kubernetes-evolution-of-an-it-revolution/#366fcb4554e1.

33. CVE Details. *CVE Details.* "Kubernetes: List of security vulnerabilities." Last accessed on 28 November 2018 at https://www.cvedetails.com/vulnerability-list/vendor_id-15867/product_id-34016/Kubernetes-Kubernetes.html.

34. Steven J. Vaughan-Nichols. (3 December 2018). *ZDNet.* "Kubernetes' first major security hole discovered." Last accessed on 3 December 2018 at https://www.zdnet.com/article/kubernetes-first-major-security-hole-discovered/.

35. Security Center. (12 June 2018). *KromTech Security Center.* "Cryptojacking invades cloud. How modern containerization trend is exploited by attackers." Last accessed on 28 November 2018 at https://kromtech.com/blog/security-center/cryptojacking-invades-cloud-how-modern-containerization-trend-is-exploited-by-attackers.

36. Trend Micro. *Trend Micro Security Intelligence Blog.* "Threat Morphosis: The Shifting Motivations Behind Digital Threats." Last accessed on 13 November 2018 at http://blog.trendmicro.com/threat-morphosis/.

37. Brian Krebs. (1 October 2016). *Krebs on Security.* "Source Code for IoT Botnet 'Mirai' Released." Last accessed on 28 November 2018 at https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.

38. Trend Micro. (13 September 2016). *Trend Micro Security News.* "Linux Security: A Closer Look at the Latest Linux Threats." Last accessed on 28 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/linux-security-a-closer-look-at-the-latest-linux-threats.

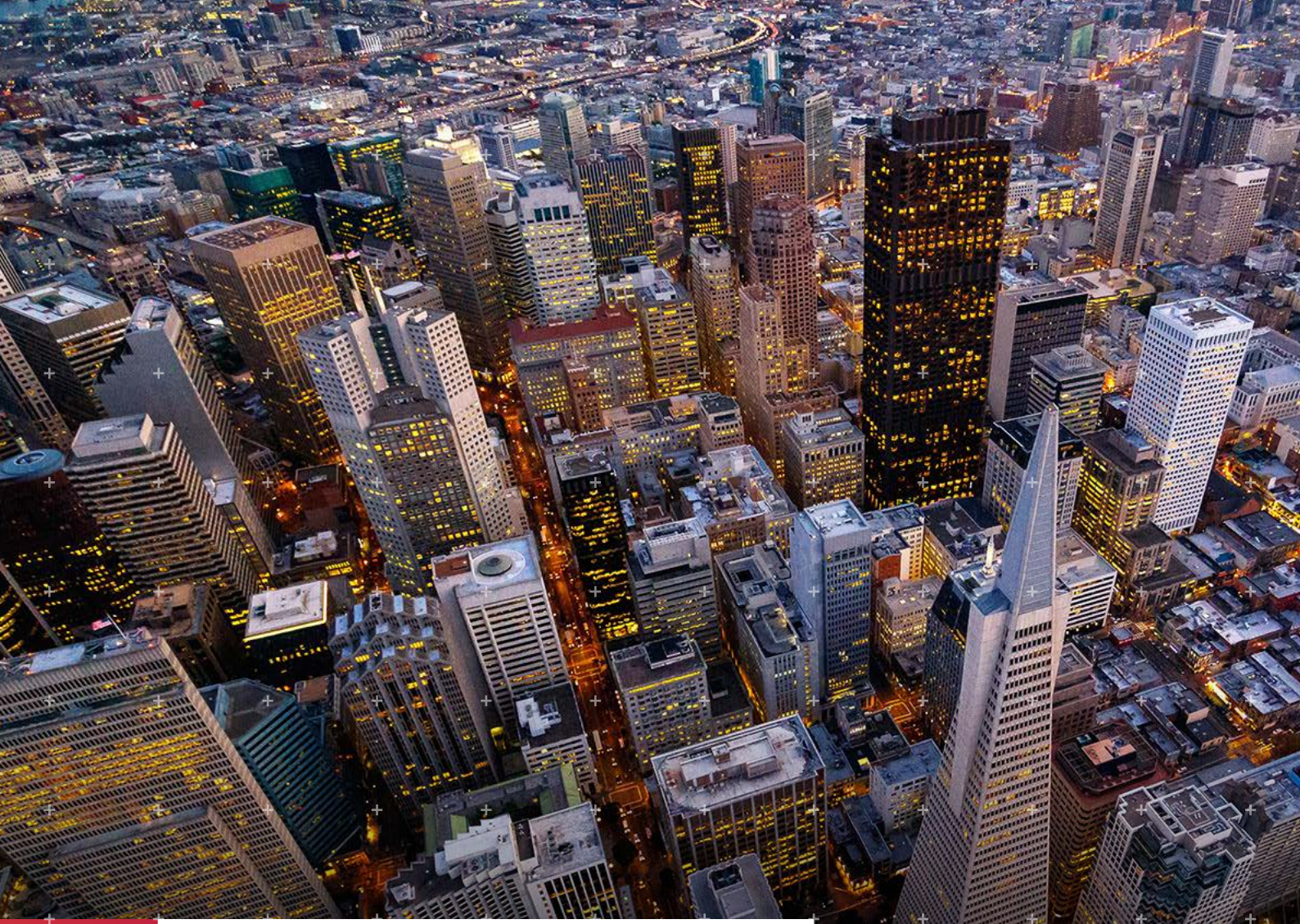
39. Spencer Hsieh. (5 October 2018). *Virus Bulletin.* "Security issues of IoV devices." Last accessed on 28 November 2018 at https://www.virusbulletin.com/conference/vb2018/abstracts/security-issues-iov-devices/.

40. Christina Farr and Jillian D'Onfro. (23 July 2018). *CNBC.* "Google is mulling a new market for Nest smart home products: seniors." Last accessed on 13 November 2018 at https://www.cnbc.com/2018/07/20/google-nest-senior-living-aging.html.

41. McCall Robison. (15 November 2018). *MarketWatch.* "These common scams target seniors—how to avoid them." Last accessed on 28 November 2018 at https://www.marketwatch.com/story/these-common-scams-target-the-elderlyhow-to-avoid-them-2018-11-15.

42. Trend Micro. (11 April 2018). *Trend Micro Security News.* "Threats to Voice-Based IoT and IIoT Devices." Last accessed on 28 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/threats-to-voice-based-iot-and-iiot-devices.

43. Jon Oltsik. (11 January 2018). *CSO Online.* "Research suggests cybersecurity skills shortage is getting worse." Last accessed on 13 November 2018 at https://www.csoonline.com/article/3247708/security/research-suggests-cybersecurity-skills-shortage-is-getting-worse.html.



Dedicato a Raimund Genes (1963-2017)

TREND MICRO™ | research

**TREND MICRO™ RESEARCH**

Trend Micro, leader globale nel settore della cybersecurity, aiuta a rendere il mondo un posto più sicuro per lo scambio delle informazioni digitali.

Trend Micro Research è a cura di esperti con la passione di scoprire nuove minacce, condividere informazioni chiave e sostenere l'impegno per fermare i cyber criminali. Il nostro team internazionale contribuisce all'identificazione di milioni di minacce ogni giorno, guida il settore del rilevamento delle vulnerabilità e pubblica ricerche innovative relative alle nuove tecniche di attacco. Lavoriamo in continuazione per anticipare le nuove minacce e produrre materiale di ricerca utile.

www.trendmicro.com