Cyber-Security: cosa ci aspetta nel 2019?

Nov 29, 2018 Marco Schiaffino Hacking, In evidenza, Malware, Minacce, News, RSS, Scenario 0

Intelligenza artificiale, attacchi alla cloud e ai sistemi di assistenza vocale. Per gli esperti di McAfee il prossimo anno proporrà minacce inedite.

Il 2018 si avvia alla conclusione ed è normale che ci si scateni nelle previsioni per il prossimo anno. Un hobby che nel settore della sicurezza informatica si traduce immediatamente in previsioni catastrofiche.

Visto che l'esercizio è comunque divertente (e in molti casi si finisce per azzeccarci) preferiamo non tirarci indietro e cominciare da subito a rendere conto di ciò che gli esperti di sicurezza si aspettano di vedere nel 2019.

I primi a cimentarsi nelle previsioni sono i ricercatori di **McAfee**, che hanno pubblicato un post sul blog della società di sicurezza in cui elencano le possibili minacce in arrivo per il nuovo anno.

La prima preoccupazione riguarda **l'ecosistema del cyber-crimine**, che secondo gli esperti di McAfee potrebbe evolvere e irrobustirsi nei prossimi 12 mesi.

Il tema non è nuovo: già negli ultimi anni, infatti, lo scambio di know-how e la compravendita di malware nei bassifondi di Internet è uno degli aspetti che ha alimentato il fenomeno della pirateria informatica a livello globale.

Gli strumenti di hacking, così come i singoli exploit,

circolano con una facilità disarmante e possono essere usati da chiunque abbia la possibilità di recuperarli e le competenze per trasformarli in malware.

In particolare, però, le preoccupazioni si concentrano sul traffico di accessi attraverso account di **Remote Desktop Protocol (RDP)** che vengono venduti o scambiati sui forum di hacking o nel Dark Web e utilizzati spesso per portare avanti campagne mirate che utilizzano ransomware.

Non solo: i forum attivi nei bassifondi di Internet secondo McAfee saranno anche il luogo di scambio di informazioni sulle **nuove vulnerabilità nel settore mobile**, un ambito in cui i cyber-criminali stanno concentrando la loro attenzione e che nel 2018 è risultato particolarmente fruttifero.

Da un punto di vista più tecnico, ciò che ci si aspetta per il futuro prossimo è l'impiego anche da parte dei "bad guys" dell'intelligenza artificiale.

La tecnologia, finora appannaggio degli esperti di sicurezza e utilizzata principalmente per individuare con maggiore precisione e tempestività le nuove minacce, ha infatti anche un altro possibile utilizzo: quello di mettere a punto **tecniche di evasione più sofisticate e complesse** rispetto a quelle a cui siamo abituati.

Secondo gli esperti, quello degli strumenti progettati per aggirare gli antivirus rischia di diventare un vero e proprio mercato che sfrutta i sistemi di intelligenza artificiale per mettere a punto strumenti di evasione che vengono poi venduti al mercato nero.

L'altra tendenza che ci si aspetta subisca una crescita esponenziale è quella della differenziazione delle modalità di attacco. Se fino a oggi ci siamo abituati a poter classificare gli attacchi in base a categorie "fisse", come ransomware, trojan, phishing e simili, in futuro la tendenza sarà quella di "mixare" le tecniche, partendo dalla prima compromissione

per poi adottare payload diversi a seconda delle situazioni.

Fino a qui ci siamo occupati della “normale” criminalità informatica, ma gli analisti prevedono anche un’espansione che andrà a coprire nuovi settori che fino a oggi sono stati interessati solo marginalmente dagli attacchi.

Un esempio? **La possibilità che i pirati informatici avviino campagne di sabotaggio dei brand commerciali, sulla sica di quanto accaduto negli ultimi mesi nel caso degli appuntamenti elettorali**.

Una campagna di disinformazione (o un bombardamento di fake news) che prende di mira un brand commerciale ha effetti potenzialmente devastanti e nell’ottica di chi agisce in un quadro di “attacco su commissione” rappresenta un possibile business che in futuro potrebbe diventare un vero problema.

Tornando agli scenari conosciuti, McAfee prevede un aumento esponenziale degli attacchi che mirano all’acquisizione di dati conservati nella cloud. Il ragionamento su cui si basa la previsione è semplice: stando alle ricerche della società di sicurezza, **il 21% dei dati conservati su cloud sono**

rappresentati da informazioni “sensibili” il cui furto può essere monetizzato facilmente.

Un ragionamento simile riguarda il settore dell’IoT, in cui è probabile che gli attacchi crescano allo stesso (forsennato) ritmo con cui crescono il numero di dispositivi della Internet of Things sul mercato. Tanto più che le vulnerabilità e gli exploit per IoT (si veda il grafico qui sotto) sono in costante crescita.

L’elemento di novità, stando al report, potrebbe riguardare gli attacchi rivolti agli assistenti vocali (in primis quelli di **Apple e Google**) la cui diffusione sta aumentando di pari passo con la diffusione dei dispositivi “smart”.

La logica, qui, è quasi banale: puntando direttamente al sistema di controllo che gestisce tutti i dispositivi, i pirati prenderebbero una sorta di “scorciatoia” che gli permetterebbe di compromettere l’intero sistema in un solo colpo.

Quante di queste previsioni si avvereranno? Difficile dirlo, ma in passato gli esperti che si sono lasciati andare a questo esercizio non hanno sbagliato di molto. Eventuali errori, poi, in questo caso si trasformerebbero in semplici sospiri di sollievo.

Please follow and like us:

AI di nuova generazione contro le tecniche di mimetizzazione dei malware Smantellata una mega-frode pubblicitaria che sfruttava 2 milioni di PC

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2018/11/29/cyber-security-cosa-ci-aspetta-nel-2019/