X-Force Exchange: la Threat Intelligence di IBM diventa open per meglio combattere i cyber attacchi

IBM annuncia la nuova piattaforma per la condivisione delle minacce informatiche

Milano - 23 apr 2015: IBM ha annunciato che renderà disponibile la sua vasta libreria di dati di security intelligence tramite IBM X-Force Exchange, una nuova piattaforma di condivisione delle informazioni sulle minacce informatiche. Questa piattaforma collaborativa consente di accedere a dati – di IBM e di terze parti - relativi a minacce alla sicurezza informatica. Tra questi dati, immediatamente fruibili, vi sono anche gli indicatori in tempo reale di attacchi in corso, importanti per difendersi dai crimini informatici. La necessità di disporre di informazioni fidate sulle minacce è più che mai sentita, considerato che l'80 percento dei cyber-attacchi è sferrato da una criminalità informatica altamente organizzata, in cui dati, strumenti e competenze sono ampiamente condivisi[1]. Se gli hacker si sono "mobilitati", non altrettanto è avvenuto per i loro bersagli. Per combattere gli hacker, la maggior parte (65 percento) dei team aziendali responsabili della sicurezza informatica utilizza diverse fonti di informazioni esterne, fidate e non[2].

X-Force Exchange si basa sulla security intelligence di vasta scala di IBM e sull'ampio portafoglio di offerta di IBM continuamente aggiornato grazie ai dati rilevati dalla Ricerca, a tecnologie come Qradar, all'esperienza fatta con migliaia di clienti al mondo e alle competenza di una rete mondiale di analisti e di esperti degli IBM Managed Security Services. Grazie alla infrastruttura cloud open su cui poggia, gli utenti di X-Force exchange potranno collaborare e accedere a svariate fonti di dati, incluse:

- uno dei cataloghi delle vulnerabilità più grandi e completi del mondo;
- informazioni sulle minacce basate sul monitoraggio di oltre 15 miliardi di eventi giornalieri legati alla sicurezza;
- intelligence sulle minacce causate da malware e provenienti da una rete di 270 milioni di endpoint;
- informazioni sulle minacce basate su oltre 25 miliardi di pagine e immagini web;
- Intelligence approfondita su oltre 8 milioni di attacchi di tipo spam e phishing;
- dati sulla reputazione basati su quasi 1 milione di indirizzi IP malevol

Oggi X-Force Exchange conta oltre 700 terabyte di dati grezzi aggregati forniti da IBM. Questo volume di dati continuerà a crescere, ad essere aggiornato e condiviso, dal momento che la piattaforma può aggiungere fino a un migliaio di indicatori di malware all'ora. Questi dati comprendono informazioni in tempo reale, cruciali per contrastare i crimini informatici.

"La piattaforma IBM X-Force Exchange permetterà la collaborazione nella scala richiesta per affrontare la

rapida crescita di minacce sempre più sofisticate come quelle che le aziende d'oggi si trovano a fronteggiare" afferma Brendan Hannigan, General Manager, IBM Security. "Aprendo il nostro network mondiale di ricerca, clienti, tecnologie ed esperti in ambito security avremo la leadership nella lotta contro la criminalità informatica. In questo ruolo coinvolgeremo i settori d'industria affinchè si uniscano al nostro impegno per condividere la loro intelligence, accelerando così la formazione di reti e di relazioni necessarie a combattere gli hacker".

Condivisione open, automatizzata e *social* delle minacce

Creato da IBM Security, IBM X-Force Exchange è una nuova piattaforma basata su cloud che permette alle organizzazioni di collaborare con facilità in merito agli incidenti di sicurezza e beneficiare dei contributi costantemente apportati dagli esperti di IBM e dai membri della community. Dal lancio della versione beta di X-Force Exchange, numerosi "early adopter" si sono già uniti alla community.

Grazie alla disponibilità in tempo reale, gratuita e condivisa della threat intelligence di IBM, gli utenti possono individuare e contribuire ad arrestare le minacce tramite:

- un'interfaccia *social* collaborativa, per interagire facilmente e convalidare le informazioni derivate da altri operatori del settore, analisti e ricercatori;
- volumi di informazioni di terze parti, continuamente approfondite e ampliate di pari passo con la crescita della base di utenti della piattaforma;
- uno strumento di raccolta, per organizzare e annotare facilmente i risultati, portando in primo piano le informazioni prioritarie;
- accesso aperto basato sul web, pensato per gli analisti e i ricercatori della sicurezza;
- una libreria di API per agevolare le query programmatiche tra la piattaforma, le macchine e le applicazioni, consentendo alle aziende di rendere operative le informazioni sulle minacce e intervenire.

All'interno della piattaforma, IBM prevede inoltre di supportare STIX e TAXII, standard emergenti per la condivisione automatizzata della threat intelligence, per estrarre e condividere con facilità le informazioni da e verso la piattaforma, oltre a integrarle senza soluzione di continuità nei sistemi di sicurezza esistenti.

Contestualizzare le minacce informatiche

Per la prima volta, attraverso questa piattaforma le organizzazioni possono interagire direttamente con gli analisti e i ricercatori della sicurezza di IBM, oltre che con gli altri operatori del settore, per validare risultati e renderli disponibili alle altre aziende che combattono i crimini informatici.

Ad esempio, un ricercatore potrebbe scoprire un nuovo dominio dannoso, segnalandolo come malevolo all'interno della piattaforma. Da qui, un analista di un'altra azienda potrebbe trovare questo dominio nella sua rete e, attraverso la piattaforma, decidere di consultarsi con altri analisti ed esperti per convalidarne il pericolo. L'analista potrebbe poi applicare le regole di blocco in merito alla presenza digitale della propria azienda, arrestando il traffico malevole e - attraverso la piattaforma - avvertire rapidamente il direttore della sicurezza delle informazioni (CISO) della minaccia. Il CISO aggiungerebbe poi questa fonte di traffico malevole nella lista pubblica presente sulla piattaforma, condividendola con gli altri operatori del settore, per contenere e arrestare rapidamente la minaccia prima che possa infettare altre aziende.

Per ulteriori informazioni, visitare il sito http://xforce.ibmcloud.com

IBM Security

La piattaforma IBM per la sicurezza fornisce security intelligence per aiutare le imprese a proteggere in modo olistico collaboratori, dati, applicazioni e infrastruttura. IBM offre soluzioni per gestione delle identità e degli accessi, gestione delle informazioni e degli eventi di sicurezza, sicurezza di database, sviluppo applicativo, gestione del rischio, gestione degli endpoint, protezione dalle intrusioni di 'next generation' e molto altro ancora. IBM gestisce una delle maggiori organizzazioni al mondo di ricerca e sviluppo in ambito security, e un'altrettanto vasta organizzazione globale per il delivery dei servizi di sicurezza.
Per ulteriori informazioni, visitate il sito www.ibm.com/security, seguite @IBMSecurity su Twitter, oppure visitate il blog di IBM Security Intelligence.

1. UNODOC Comprehensive Study on Cybercrime 2013
2. ESG: http://bit.ly/1xzTmUW
