

Rapporto IBM X-Force: nel 2018 i profitti dei criminali informatici arrivano dal cryptojacking mentre i ransomware sono in declino

Il rapporto rileva, inoltre, che oltre la metà degli attacchi informatici non sono più basati su malware; aumentano le campagne mirate a compromettere i sistemi di posta elettronica aziendali

Cambridge, MA - 26 feb 2019: IBM Security ha annunciato i risultati del suo rapporto annuale [2019 IBM X-Force Threat Intelligence Index](#), da cui è emerso che l'aumento delle misure di sicurezza e una sempre maggiore consapevolezza spingono i criminali informatici a modificare le tecniche di attacco, mossi come sempre dalla ricerca del migliore ritorno sull'investimento. Il rapporto descrive due importanti cambiamenti: una minore dipendenza dal malware e un sorprendente abbandono graduale del ransomware.

IBM X-Force ha notato un significativo calo del ransomware utilizzato negli attacchi. Infatti, i ricercatori di spam di IBM hanno rilevato una sola campagna di ransomware nel 2018 proveniente dalla più grande botnet di distribuzione di spam malware al mondo, Necurs. IBM X-Force ha anche osservato che il numero di attacchi di cryptojacking - ovvero l'utilizzo illegale della capacità elaborativa del computer di un individuo o di un'organizzazione per estrarre criptovalute - è stato, nel 2018, quasi il doppio del numero attacchi di ransomware. Con il prezzo di criptovalute, come i bitcoin, che ha toccato un massimo di [quasi \\$20.000 nel 2018](#), gli attacchi a basso rischio/basso sforzo rivolti in segreto alla potenza di calcolo delle vittime erano considerati più redditizi.

Inoltre, l'IBM X-Force Threat Intelligence Index ha rilevato che i criminali informatici stanno cambiando le loro tecniche fraudolente per ottenere profitti illegali. IBM X-Force ha osservato un aumento negli strumenti che violano il sistema operativo, rispetto all'uso di malware. Oltre la metà degli attacchi informatici (57%) hanno sfruttato comuni applicazioni di amministrazione, come PowerShell e PsExe, per eludere il rilevamento, mentre gli attacchi di phishing mirati rappresentavano quasi un terzo (29%) degli attacchi.

L'IBM X-Force Threat Intelligence Index comprende analisi e osservazioni di dati che derivano dal monitoraggio giornaliero in 130 paesi. I dati sono quelli raccolti e analizzati attraverso diverse fonti, quali X-Force IRIS, X-Force Red, IBM Managed Security Services, oltre a quelli provenienti dalle informazioni sulle violazioni divulgate pubblicamente. IBM X-Force utilizza migliaia di trappole per lo spam in tutto il mondo, monitora quotidianamente decine di milioni di attacchi di spam e phishing e analizza miliardi di pagine web e di immagini al fine di rilevare attività fraudolente e tentativi di violazione dei marchi.

Tra i risultati emersi ricordiamo:

- **Segnalazioni di vulnerabilità in aumento:** quasi un terzo (42.000) di tutte le 140.000 vulnerabilità rilevate da IBM X-Force negli ultimi trent'anni sono state segnalate solo negli ultimi tre anni. Infatti, IBM X-Force Red rileva in media 1.440 vulnerabilità esclusive per ciascuna organizzazione monitorata.
- **Gli errori di configurazione continuano ad affliggere le organizzazioni:** gli incidenti di errata configurazione divulgati pubblicamente aumentano del 20% all'anno. È interessante notare che c'è stata una diminuzione del 52% nel numero di record di dati compromessi a causa di questo vettore di minacce.
- **Gli attacchi BEC sono quelli che rendono maggiormente:** le campagne di phishing hanno sfruttato massicciamente le truffe di tipo [Business Email Compromise \(BEC\)](#), che hanno rappresentato il 45% degli attacchi di phishing tracciati da X-Force.
- **Il settore dei trasporti emerge come quello da tenere d'occhio (per gli attacchi informatici):** il settore dei trasporti è diventato il secondo settore più soggetto ad attacchi nel 2018, salendo dal 10o posto del 2017.

“Se guardiamo al calo nell’uso del malware, al progressivo abbandono del ransomware e all’aumento delle campagne mirate, tutte queste tendenze ci dicono che il ritorno sull’investimento è il vero fattore motivante per i criminali informatici. Tuttavia, le iniziative per distruggere gli avversari e rendere i sistemi più impenetrabili stanno funzionando. Con 11,7 miliardi di dati violati o rubati negli ultimi tre anni, lo sfruttamento delle Informazioni Personali Identificabili (PII) per realizzare profitti illeciti richiede maggiori conoscenze e risorse, spingendo i criminali a esplorare nuovi modelli illeciti per fare profitto e aumentare il ritorno dell’investimento” ha dichiarato Wendi Whitmore, Global Lead, IBM X-Force Incident Response and Intelligence Services (IRIS). “Uno dei prodotti più allettanti è il potere di elaborazione legato all'emergere delle criptovalute. Ciò ha portato ad azioni segrete di highjacking delle reti aziendali e dei dispositivi dei consumatori alla ricerca di queste valute digitali.”

Aumento dell’uso criminale di PowerShell

La crescente consapevolezza dei problemi di sicurezza informatica e controlli di sicurezza più rigorosi stanno rendendo più difficile per i criminali informatici fare presa sui sistemi oggetto dei loro attacchi. Pertanto, l’uso di software malevolo negli attacchi sembra essere in declino. Più della metà (57%) degli attacchi analizzati da X-Force nel 2018 ha rivelato che gli autori delle minacce non utilizzavano malware residente nei file system. Coloro che hanno fatto un uso più frequente del malware erano grandi bande di criminali informatici e gruppi responsabili di minacce del tipo APT (Advanced Persistent Threat).

Nei casi in cui le reti sono state compromesse dagli hacker, IBM X-Force ha rilevato un importante cambiamento nelle tecniche dei criminali informatici che, per raggiungere gli obiettivi, hanno violato gli strumenti dei sistemi operativi esistenti, anziché utilizzare malware. Il fulcro di queste tecniche è l’uso avanzato di PowerShell, uno strumento integrato nel sistema operativo, in grado di eseguire codice dalla memoria e fornire accesso amministrativo direttamente al core di un dispositivo. IBM X-Force Incident Response and Intelligence Services (IRIS) ha, inoltre, osservato che gli hacker eseguono query WMIC (Windows Management Interface Command), che vengono successivamente utilizzate per automatizzare l’esecuzione remota di comandi e script PowerShell, tra le altre funzioni progettate per eseguire query, effettuare ricerche in database, accedere alle directory degli utenti e connettersi a sistemi di interesse.

I criminali informatici attaccano i sistemi per mero profitto

I criminali informatici non sono tipi disposti a spendere soldi per hardware costoso o per cercare criptovaluta in modo legale. Al contrario, hanno sviluppato vari strumenti e tattiche per infettare sia server aziendali che singoli utenti con malware che cerca soldi e che fa il lavoro sporco per loro. A loro volta, queste infezioni compromettono la potenza di elaborazione, con conseguente aumento dell’utilizzo della CPU e rallentamento dei dispositivi. Questa tendenza al cryptojacking sta praticamente esplodendo e i criminali informatici ne traggono vantaggio, in quanto i due più comuni vettori di infezione sono il phishing e l’iniezione di codice in siti web con controlli di sicurezza deboli.

IBM X-Force ha scoperto che gli attacchi illeciti di cryptojacking sono in aumento mentre il ransomware sembra essere in declino. Nel corso del 2018, i tentativi di installare ransomware sui dispositivi monitorati da X-Force nel 4° trimestre (ottobre-dicembre) sono diminuiti a meno della metà (45%) dei tentativi effettuati nel 1° trimestre. Invece, gli attacchi di tipo cryptojacking sono più che quadruplicati, raggiungendo il 450% nello stesso intervallo di tempo.

Settore dei trasporti sempre più nel mirino della criminalità informatica

I criminali informatici non stanno solo cambiando la modalità degli attacchi, ma anche i bersagli. Il settore finanziario è rimasto il settore più attaccato del 2018 e rappresenta il 19% di tutti gli attacchi osservati da IBM X-Force IRIS. Tuttavia, il settore dei trasporti, che l'anno scorso non è arrivato nemmeno nei primi 5 posti, è diventato il secondo settore più attaccato nel 2018, anno in cui i tentativi di attacco si sono triplicati rispetto all'anno precedente.

Non si tratta solo del volume degli attacchi, ma anche del calibro delle vittime. X-Force ha osservato più dichiarazioni pubbliche nel 2018 rispetto agli anni precedenti nel settore dei trasporti. Tali dichiarazioni probabilmente hanno incoraggiato gli hacker, poiché potrebbero denotare che queste società sono vulnerabili agli attacchi informatici e che possiedono dati preziosi come dati dei clienti, informazioni sulle carte di pagamento, informazioni personali identificabili (PII) e account di fidelizzazione.

Il rapporto contiene i dati raccolti da IBM Security tra il 1° gennaio 2018 e il 31 dicembre 2018 per fornire informazioni approfondite sul panorama globale delle minacce e informare i professionisti della sicurezza riguardo alle minacce più rilevanti per le loro organizzazioni. Per scaricare una copia dell'IBM X-Force Threat Index per il 2019, visita: <https://www.ibm.com/security/data-breach/threat-intelligence>.

Se sei interessato, iscriviti al webinar dell'IBM X-Force Threat Intelligence Index che si terrà il 29 marzo 2019. Questo il link per l'iscrizione <https://bit.ly/2E2KYSb>

Informazioni su IBM Security

IBM Security offre uno dei portfolio più completi e integrati di prodotti e servizi per la protezione aziendale. Il portfolio, supportato dal team di ricerca di fama mondiale IBM X-Force®, consente alle organizzazioni di gestire con efficacia il rischio e difendersi dalle minacce emergenti. IBM dirige una delle organizzazioni di ricerca, sviluppo e delivery di soluzione di sicurezza più grandi al mondo, monitora 70 miliardi di eventi di security al giorno in più di 130 Paesi e ha ottenuto oltre 10.000 brevetti di sicurezza. Per maggiori informazioni, visita il sito www.ibm.com/security, segui @IBMSecurity su Twitter o visita il [blog di IBM Security Intelligence](#).

Contatti

Claudia Ruffini

IBM Media Relations +393356325093cla@it.ibm.com

Alessandro Ferrari

IBM Media Relations +393484554535ale_federferrari@it.ibm.com
