

IBM X-Force: furto di credenziali e vulnerabilità del software sono le armi usate contro le aziende nel 2019

I brand consumer tech si sono trovati nel fuoco incrociato degli attacchi di phishing; gli errori di configurazione dei sistemi sono per l'85% causa di esposizione al rischio; forte il legame tra trojan bancari e ransomware

Cambridge, MA - 11 feb 2020: IBM Security ha rilasciato oggi **[l'IBM X-Force Threat Intelligence Index 2020](#)**, che evidenzia come le tecniche dei criminali informatici continuino a evolvere dopo decenni di attività che hanno permesso l'accesso a decine di miliardi di record di dati, aziendali e personali, e di fare breccia attraverso centinaia di migliaia di vulnerabilità del software. Secondo il rapporto, nel 60% dei casi le violazioni di rete sono state realizzate o attraverso l'utilizzo di credenziali di accesso precedentemente rubate o a causa di vulnerabilità note del software, consentendo ai criminali informatici di operare senza necessità di ricorrere a tecniche fraudolente.

L'X-Force Threat Intelligence Index di IBM indica i fattori che contribuiscono all'evoluzione delle tecniche, analizzando i tre principali vettori da cui partono gli attacchi:

- Il phishing si è rivelato un vettore di successo delle violazioni nel 31% degli incidenti identificati, rispetto al 50% del 2018.
- Lo *scanning* e l'*exploiting* delle vulnerabilità sono stati identificati nel 30% degli incidenti osservati nel 2019, rispetto all'8% dell'anno precedente. A tal proposito, le vulnerabilità già note in Microsoft Office e Windows Server Message Block sono state sfruttate in modo significativo anche nel 2019.
- Nel 29% degli attacchi informatici analizzati, l'uso di credenziali di accesso rubate è sempre più frequente. Secondo il report, nel 2019 sono stati compromessi grazie a questa risorsa oltre 8,5 miliardi di file, segnando un aumento del 200% delle violazioni rispetto agli anni precedenti.

"Oggi la mole di record esposti a rischio rivela come gli hacker non abbiano bisogno di ricorrere a metodi sofisticati per sferrare un attacco informatico ma necessitino solo delle credenziali di accesso con cui entrare", ha affermato Wendi Whitmore, Vice President, IBM X-Force Threat Intelligence. "Misure di protezione, come l'autenticazione a più fattori e il single sign-on, sono fondamentali per la cyber-resiliency delle organizzazioni e la protezione e la privacy dei dati degli utenti".

IBM X-Force ha condotto le proprie ricerche monitorando più di 70 miliardi di eventi giornalieri nell'area della security, in oltre 130 Paesi. I dati sono stati raccolti da più fonti - tra cui X-Force IRIS, X-Force Red, IBM Managed Security Services - per poi essere esaminati. IBM X-Force fa girare migliaia di spam traps in tutto il mondo e monitora quotidianamente decine di milioni di attacchi spam e phishing, oltre ad analizzare miliardi di pagine Web e immagini per rilevare attività fraudolente e abusi nei confronti dei brand.

Le principali evidenze:

- **Configure it Out:** l'analisi di IBM ha rilevato che nel corso del 2019 la violazione di 7 miliardi di record, su

un totale di oltre 8.5 miliardi, è imputabile ad una non corretta configurazione dei server cloud o errate configurazioni di sistema. Si tratta di un brusco cambio di rotta rispetto al 2018 quando i record violati per queste cause costituivano il 50% del totale.

- **Banking on Ransomware:** alcuni dei trojan più attivi nel settore bancario, come TrickBot, sono stati oggetto di un monitoraggio intenso da parte degli hacker che li hanno usati per preparare attacchi ransomware. In effetti, il nuovo codice utilizzato dai trojan bancari e dai ransomware ha superato le classifiche rispetto ad altre varianti di malware discusse nel rapporto.

- **Fiducia nelle tecnologie per il phishing :** dalla ricerca IBM X-Force emerge che i brand tech, dei social media e dello streaming di contenuti siano nella "Top 10" dei marchi contraffatti dai cybercriminali nei loro tentativi di phishing. Ciò denota una crescente fiducia nei confronti dei brand tech, rispetto a quelli del retail e della finanza, storicamente affidabili. Tra i primi dieci brand colpiti dal fenomeno del cybersquatting compaiono Google, YouTube e Apple.

L'evoluzione degli attacchi ransomware

Secondo il report, gli attacchi ransomware a livello globale sono indirizzati sia al settore pubblico sia a quello privato, inoltre il fenomeno delle attività ransomware nel 2019 ha registrato un incremento. Il Team IBM X-Force, costantemente impegnato nel fronteggiare le attività ransomware in 13 diversi settori in tutto il mondo, evidenzia come questi attacchi siano perpetrati indistintamente in ogni settore.

Mentre lo scorso anno oltre [100 enti governativi statunitensi](#) sono stati colpiti da attacchi ransomware, nel 2019 sono stati significativamente compromessi i settori retail e manifatturiero, ma anche l'industria dei trasporti. Ciò è dovuto al fatto che le società operanti in questi settori sono interessanti per i criminali cyber in quanto gestiscono informazioni preziose, come i dati personali dei clienti, che risultano facilmente monetizzabili e spesso si avvalgono di tecnologie datate.

Nell'80% dei tentativi di attacchi ransomware rilevati, gli hacker hanno sfruttato le vulnerabilità di Windows Server Message Block. Si tratta della tattica già utilizzata per propagare [WannaCry](#), il ransomware che nel 2017 ha paralizzato le aziende in 150 Paesi. I [costi](#) sostenuti dalle organizzazioni vittime di attacchi di ransomware nel corso del 2019 sono superiori ai 7,5 miliardi di dollari, e per il 2020 si prevede che questi crimini informatici non si arresteranno. Il report di IBM, in collaborazione con [Intezer](#), informa che è stato intercettato un nuovo codice malware nel 45% dei trojan bancari e nel 36% dei ransomware. Ciò indica che gli hacker sono costantemente impegnati nella creazione di nuovi codici per non essere identificati.

Allo stesso tempo, IBM X-Force ha osservato una forte relazione tra ransomware e trojan bancari. Questi ultimi vengono utilizzati per ottenere l'accesso ad una rete infetta, dove viene successivamente inoculato il ransomware. Ad esempio, Trickbot, che secondo il report è il malware più attivo in ambito finanziario, è sospettato di diffondere Ryuk su reti aziendali, mentre altri trojan bancari, come QakBot, GootKit e Dridex, si stanno anche diversificando per varianti di ransomware.

Contraffazioni di brand tech e social tra gli obiettivi del phishing

Con l'accrescere della consapevolezza da parte degli utenti in merito alla dannosità delle e-mail di phishing, le

tecniche di phishing stesso diventano sempre più sofisticate.

In collaborazione con [Quad9](#), IBM ha rilevato la tendenza da parte degli hacker a impossessarsi in modo illegale dei profili dei brand consumer tech per indurre gli utenti a cliccare link malevoli - a social media o a contenuti in streaming - che nascondono azioni di phishing

Tra i primi dieci brand contraffatti, sei avevano domini di Google e YouTube, mentre i domini Apple (15%) e Amazon (12%) sono stati violati soprattutto per i loro dati monetizzabili. IBM X-Force, infatti, rileva proprio nell'elevata opportunità di monetizzazione la causa degli attacchi verso tali brand.

Anche Facebook, Instagram e Netflix sono nella lista dei primi dieci brand che hanno subito il furto di identità digitale sui social media, anche se in misura inferiore. Ciò può essere dovuto al fatto che questi siti, in genere, non contengono dati direttamente monetizzabili. Poiché gli hacker fanno spesso affidamento sul riutilizzo delle stesse credenziali per ottenere l'accesso agli account più redditizi, IBM X-Force ritiene che il riutilizzo frequente delle password sia una delle principali cause di vulnerabilità di questi brand, bersaglio per gli hacker. In effetti, il [Future of Identity Study](#) di IBM ha scoperto che il 41% dei millennial intervistati riutilizza la stessa password più volte e la generazione Z detiene in media solo cinque password, evidenziando l'abitudine molto diffusa tra i più giovani a riutilizzare le medesime password.

Riuscire a identificare domini falsificati può essere estremamente difficile, ed è proprio questa la complessità su cui fanno affidamento i criminali informatici. Con un totale di quasi 10 miliardi di account (Nota 1), i primi 10 marchi falsificati elencati nel rapporto offrono agli hacker un ampio target di potenziali destinatari di attacchi, aumentando la probabilità che un utente ignaro clicchi su un link apparentemente innocuo, ma in realtà contraffatto.

Altri dati chiave rilevati dal report

- Il settore **Retail tra i più presi di mira**: da quanto si evince nel report, il settore retail è stato il secondo maggiormente attaccato nel corso del 2019, subito dopo il settore bancario. La scorsa estate [sono stati](#) ben 80 i siti e-commerce compromessi da MageCart, il virus progettato per il furto di credenziali, dati delle carte di credito e altre informazioni sensibili. Secondo IBM, il settore retail è stato vittima di attacchi ransomware.
- **Gli attacchi ai sistemi di controllo industriale (ICS) e l'operational technology (OT) salgono alle stelle**, registrando una crescita del 2000% rispetto agli ultimi tre anni. Gli attacchi informatici sono stati perpetrati a causa di vulnerabilità rilevate nel sistema SCADA e nell'hardware utilizzato nei sistemi di controllo industriale (ICS), così come attraverso il password-spraying, la tecnica volta a tentare di accedere a più utenze con semplici password comunemente diffuse.
- **Il Nord America e l'Asia sono le aree maggiormente colpite**: queste regioni hanno registrato il maggior numero di attacchi e hanno subito le maggiori perdite di dati nell'ultimo anno, con -rispettivamente - oltre 5 miliardi e 2 miliardi di record violati.

Il report, che presenta i dati raccolti da IBM nel 2019, fornisce informazioni approfondite sul panorama globale delle minacce informatiche e aiuta le aziende a comprenderne i rischi le minacce emergenti per fronteggiarli al meglio. È possibile scaricare una copia di IBM X-Force Threat Index 2020, attraverso questo

link: <https://ibm.biz/downloadxforcethreatindex>

Iscriviti al webinar IBM X-Force Threat Intelligence Index 2020 martedì 18 febbraio 2020 alle 11:00

ET: <https://ibm.biz/BdqExS>

Informazioni su IBM Security

IBM Security offre un ampio portfolio di prodotti e servizi di sicurezza per le imprese, tra i più innovativi e integrati del mercato. Il portfolio, sostenuto dai risultati del team di ricerca mondiale in cyber security, IBM X-Force®, consente alle organizzazioni di gestire efficacemente i rischi e difendersi dalle minacce emergenti. IBM dispone di una delle più grandi organizzazioni mondiali in ambito security, che offre ricerca, sviluppo e servizi in oltre 130 paesi, monitora 70 miliardi di eventi di sicurezza al giorno e ha ottenuto oltre 10.000 brevetti di sicurezza in tutto il mondo. Per ulteriori informazioni, visitare www.ibm.com/security, seguire @IBMSecurity su Twitter o visitare il blog IBM Security Intelligence.

Contatti

Claudia Ruffini

IBM Media Relations +393356325093

cla@it.ibm.com

Paola Piacentini

IBM Media Relations +393351270646

paola_piacentini@it.ibm.com

<https://it.newsroom.ibm.com/2020-02-11-IBM-X-Force-furto-di-credenziali-e-vulnerabilita-del-software-sono-le-armi-usate-contro-le-aziende-nel-2019>