I malware più diffusi rimangono i ransomware, +100% nel 2018

Gli attacchi **ransomware** rimangono tra le più temibili minacce informatiche per le organizzazioni a livello mondiale, sono di gran lunga il tipo di malware più diffuso, responsabili del 39% delle violazioni dovute ai malware – il doppio rispetto a quanto segnalato lo scorso anno, protagonisti di più di 700 attacchi, e come se non bastasse, adesso questi attacchi vengono sferrati anche contro gli asset più critici delle aziende, crittografando server o database, causando quindi danni maggiori, e, di conseguenza, condannando le vittime a riscatti più elevati.

Ecco l'analisi inquietante nel mondo della sicurezza informatica presentata da **Verizon** nel suo annuale **Data Breach Investigations Report 2018**, giunto quest'anno all'undicesima edizione.

L'edizione di quest'anno che si affida ai dati forniti da 67 organizzazioni a livello mondiale, ha analizzato 53,000 attacchi e 2,216 violazioni, che hanno avuto luogo in 65 Paesi diversi.

I dati del DBIR mettono in guardia anche riguardo il cambiamento nelle dinamiche di utilizzo degli attacchi di phishing e pretexting a scopo pecuniario. Infatti, questo tipo di attacchi, che, attraverso i dipendenti, continuano ad insidiare le organizzazioni, stanno coinvolgendo ora interi reparti. Dal report emerge che le risorse umane (HR), tra i diversi settori analizzati, sono nell'occhio del ciclone, perché i criminali possono così ottenere informazioni come lo

stipendio dei dipendenti oppure informazioni relative alle tasse, ed escogitare quindi frodi, cercando di dirottare le somme dei rimborsi.

Le principali minacce

- **I ransomware sono il software malevolo più diffuso**: responsabili del 39 per cento dei casi legati ad attacchi malware analizzati quest'anno, e sono cresciuti molto rispetto alla quarta posizione, che detenevano nel DBIR 2017 (erano alla ventiduesima nel 2014). E, soprattutto, secondo i dati elaborati da Verizon, iniziano a insidiare gli asset più critici delle aziende, non più soltanto i pc. Per questo, le cifre richieste per i riscatti sono in aumento, e i cybercriminali, di fatto, traggono profitti ancora maggiori, con meno fatica.
- **Il fattore umano è ancora tra le debolezze principali:** gli attacchi di social engineering mietono ancora vittime tra i dipendenti. Il pretexting ed il phishing per l'estorsione di denaro rappresentano il 98 per cento di questi attacchi, e il 93 per cento di tutte le violazioni su cui il report ha indagato – e l'anello debole continuano ad essere le email (nel 96 per cento dei casi). Le aziende corrono un rischio tre volte più elevato di essere colpite da un attacco di social engineering che da una vera e propria vulnerabilità, rendendo inequivocabile la necessità di programmi di formazione continua in ambito cybersecurity, per tutti i dipendenti.
- **Il pretexting a scopo pecuniario mira alle HR:** il pretexting è quintuplicato rispetto a quanto rilevato dal DBIR 2017, quest'anno sono stati infatti analizzati 170 attacchi (rispetto ai 61 dell'edizione 2017). Di questi, 88 hanno mirato specificamente a dipendenti del settore HR al fine di sottrarre dati personali con i quali completare moduli per false richieste di rimborso

tasse.

- **Anche gli attacchi phishing non passano inosservati:** se, in media, il 78 per cento degli utenti l'anno scorso non è caduto nella rete del phishing, per ogni singola campagna di questo tipo il 4 per cento degli utenti cade invece nel tranello. E ad un cybercriminale serve una sola vittima per riuscire ad avere accesso ad un'intera organizzazione.
- **Gli attacchi DDoS prosperano:** gli attacchi di tipo DDoS possono colpire chiunque, e spesso sono un trucco messo in atto, sospeso e poi rimesso in funzione per mascherare altre violazioni che agiscono sullo sfondo. Sono attacchi molto potenti, ma possono essere affrontati e gestiti con la tecnica di difesa giusta.
- **La maggior parte degli hacker sono esterni alle organizzazioni:** una singola violazione può essere opera di molti hacker, e abbiamo scoperto che – il 72 per cento degli attacchi vengono perpetrati ad opera di criminali esterni, il 27 per cento è stato causato invece da soggetti interni, mentre il 2 per cento ha visto il coinvolgimento di un partner, e un ulteriore 2 per cento coinvolgeva invece diversi partner. La criminalità organizzata è ancora responsabile del 50 per cento degli attacchi analizzati.

I rischi per settore

Il report di quest'anno rivela le più temibili minacce che le aziende, settore per settore, si ritrovano a dover affrontare, e propone alcune linee guida per arginare questi rischi. I dati principali, relativi ai diversi settori, includono:

- **Istruzione** – Gli attacchi basati sul social engineering che mirano all'estorsione di dati personali sono molto frequenti, e questo bottino viene poi utilizzato per furti d'identità. Anche le ricerche più delicate sono a rischio, e lo spionaggio è alla base del 20 per cento di

questi attacchi. L'11 per cento, invece, viene sferrato a scopo ludico, non finanziario.

- **Finanza e assicurazioni** – I sistemi per la clonazione di carte di credito installati presso gli sportelli bancomat sono ancora un ottimo affare. Tuttavia, è in crescita anche la tecnica del "bancomat jackpotting", secondo la quale un software o un hardware installato in modo illecito dà comandi al bancomat, perché emetta grandi quantitativi di denaro contante. Un'altra minaccia da non sottovalutare sono gli attacchi DDoS.
- **Sanità** – Si tratta dell'unico settore in cui le minacce interne sono maggiori di quelle provenienti dall'esterno. E l'errore umano è tra i fattori di rischio più comuni.
- **Informazione** – Gli attacchi DDoS sono responsabili di più della metà (56 per cento) di quelli che colpiscono l'intero settore.
- **Settore pubblico** – Il cyberspionaggio è decisamente tra le preoccupazioni più gravi, dato che il 43 per cento delle violazioni hanno questo scopo. Nonostante questo, non sono unicamente i segreti di stato ad essere nel mirino, ma anche i dati personali.

Tra gli altri settori presi in esame dal report figurano: il settore alberghiero e della ristorazione, quello dei professionisti, della scienza e della tecnica, del settore manifatturiero e del retail.

"I ransomware sono ancora la minaccia più concreta per le aziende di qualsiasi dimensione," ha dichiarato **Bryan Sartin**, executive director security professional services di Verizon. *"Ad oggi sono infatti la forma di malware più frequente, e quella largamente più utilizzata negli ultimi anni. Le aziende, tra l'altro, devono continuare ad investire nella formazione dei dipendenti, che devono conoscere le minacce informatiche e l'effetto negativo che hanno sul brand, la reputazione e il fatturato. I dipendenti, infatti, dovrebbero*

costituire la prima linea difensiva di un’azienda, non l’anello debole della catena della sicurezza. Formazione e training continui sono essenziali, perché per esporre a questi pericoli un’intera organizzazione, è sufficiente che una sola persona apra una mail di phishing.”

https://www.key4biz.it/i-malware-piu-diffusi-rimangono-i-ransomware-100-nel-2018/218120/