Cybercrime, cosa si vende nel dark web?

Cosa succede quando la parte di nascosta del web, dove hanno luogo le transazioni più sregolate decide di rinfrescare la sua impostazione commerciale?

Le implicazioni per la cybersecurity sono sicuramente molte, un tempo il **Dark web**, per definizione, era un luogo dove la sola parola garanzia era impronunciabile: le transazioni avvenivano in un contesto di massima insicurezza, senza alcuna certezza. Oggi, mimando il successo dell'on-line retail il Dark web si è dotato di uno dei componenti chiave del successo della sua controparte legale, le garanzie. Non solo, queste piattaforme distorte di eCommerce operano su piattaforme che permettono di recensire i "prodotti", lasciare una valutazione e ottenere garanzie di acquisto, il tutto incorniciato con un'interfaccia intuitiva e responsive facilmente navigabile. Non mancano neppure elementi di customer care come FAQ, chat di supporto e dettagliate pagine di aiuto.

La valuta principale di scambio non è il dollaro e neppure lo yen, qui la fanno da padrone le cripto valute grazie alle loro caratteristiche che permettono grande anonimato e scarsa tracciabilità.

Tra la merce a disposizione al primo posto per numero di inserzioni regnano ancora gli stupefacenti, ma a breve distanza troviamo innumerevoli *hacking tools* e pacchetti di dati sensibili illegalmente ottenuti. Siamo dinnanzi a una *regolarizzazione* della delinquenza e le implicazioni per la cybersecurity sono molte.

Cybercrime commodity: i must have

Ma quali sono i programmi più popolari in vendita all'interno di queste piattaforme? Alcuni esempi delle categorie più popolari:

Tra i vari malware offerti sulle piattaforme, i più pericolosi sono sicuramente i Remove Access Trojan. Questa variante di software dannoso può mettere in condizione il pirata informatico di prendere totalmente il controllo del pc della sua vittima. Questo la rende scoperta e vulnerabile nei confronti di una pletora di potenziali crimini: dal furto di dati sensibili – dalle carte di credito, Paypal, dati di homebanking – al vero e proprio furto d'identità, ma i RAT sono anche usati per accedere alle webcam integrate che vengono sfruttate a fini di ricatto. Attenzione però, non sono solo i personal computer a essere aperti al rischio di questa infezione, alcune varianti di malware sono state in grado di contagiare anche nei dispositivi mobile che utilizzano l'OS Android.

Anche in questo caso fioriscono le offerte di programmi più o meno differenti. I target più frequenti di questi programmi, utilizzati per sottrarre password, sono i siti social e di svago come Facebook e Spotify.

Il **phishing** è sicuramente uno dei vettori di cyberattacco più diffusi, quindi non c'è da stupirsi se all'interno del Dark web esistono centinaia di inserzioni in vendita per pagine che in maniera camaleontica replicano siti di brand affermati come Netflix, Facebook, Twitter…

Oltre ai metodi già citati sono disponibili una pletora di opzioni di Hacking in vendita a prezzi inferiori ai 10 dollari: i keyloggers – software in grado di catturare tutto ciò che viene digitato sulla tastiera del PC -, vari software in grado violare reti Wifi e connessione Bluetooth e malware progettati per sottare Bitcoin.

Così come il mercato delle tecnologie IT ha sviluppato offerte in grado di soddisfare l'utente finale secondo tutte le sue necessità allo stesso modo anche il Dark Web ha sviluppato pacchetti omnicomprensivi per aspiranti truffatori. In particolare, questo è stato osservato nel mercato della falsificazione di documenti ufficiali. Sono stati creati veri e propri template Photoshop – completi di dettagliate istruzioni per l'uso – che coprono tutto il ventaglio dei documenti: carte d'identità, patenti, passaporti, bollette, fatture… Questi template sono usati in combinazione con i cosiddetti "Fullz", termine proprio dello slang degli hacker, che indica il pacchetto completo dei dettagli personali (nome, codice fiscale, data di nascita, numero di conto corrente bancario…) sottratti alla vittima di furto d'informazioni e ugualmente disponibili sul Dark web. Il risultato dell'unione di questi dati con i template (venduto appunto come soluzione completa) viene usato principalmente per commettere frodi bancarie. Ciò, in breve, è significativo di quanto si sia evoluto questo mercato "underground": il criminale intenzionato a commettere una frode può effettivamente acquisire un pacchetto completo di strumenti e istruzioni per l'uso atte a questa attività criminale.

Cybercrime commodity: un epidemia in procinto?

Quelli elencati non sono altro che alcuni semplici esempi dell'enorme business che è il cybercrime oggi. Di certo è un'utopia l'augurarsi di poter debellare completamente le attività criminose, ma alcune accortezze da parte del consumatore possono portare significativi benefici atti a scongiurare questi attacchi e mantenere la propria sicurezza. Un consiglio è quello di utilizzare, laddove possibile, un sistema autenticazione a due fattori, che assicura un'ulteriore barriera di protezione anche nel caso in cui venga sottratta la password. Un altro facile accorgimento

riguarda l’igiene delle password: una sicura non deve essere scontata, non deve richiamare al tuo nome/data di nascita o a quello dei tuoi cari, non deve essere eccessivamente corta e deve includere caratteri speciali. Il cambio di paradigma necessario per assicurarsi maggiore protezione non è solo tecnico, ma anche culturale: lo sforzo combinato deve avere luogo lungo tutta la filiera digitale per educare ed educarsi sull’importanza della sicurezza online è la vera strada per rendere inefficaci, se non solo per gli hacker più esperti, tutti gli strumenti che pullulano sulle piattaforme presenti nel Dark web.

La battaglia deve essere combattuta su due fronti: tecnico e culturale. Si è reso imperativo l’acquisto di skill, anche basilari, per affrontare le criticità della cybersecurity. Una buona strada per raggiungere questo obiettivo è quella di intraprendere corsi di formazione. Il mercato ha, fortunatamente risposto a questa necessità ed è oggi possibile prendere parte a corsi tailor made per ogni tipo di livello richiesto, dalle basi di Cybersecurity awareness a sessioni su argomenti più avanzati come l’Ethical Hacking.

Sul lato più “company”, uno dei migliori metodi, per business e provider di servizi web, di comprendere a quali rischi possono essere soggetti i propri domini, app, etc… è quello di eseguire un Vulnerability Assessment test: si tratta di un’analisi di sicurezza effettuata per identificare tutte le vulnerabilità potenziali di sistemi, pagine web, network e applicazioni. Come fare per effettuarne uno? Sono disponibili molti strumenti automatizzati.

Questi tools effettuano controlli approfonditi su ogni sistema o applicazione e riconoscono le vulnerabilità presenti. Un altro aspetto importante da considerare è la velocità di scansione. La celerità di questi tool rende possibile la scansione di un perimetro molto ampio in un periodo di tempo relativamente breve, fornendo, inoltre, un buon livello di dettaglio, questo per garantire la massima efficienza

nell’intervenire e correggere eventuali falle di cybersecurity presenti nel sistema.

https://www.key4biz.it/cybercrime-cosa-si-vende-nel-dark-web/255313/