# La grande truffa della criminalità informatica

**di Caleb Barlow –** Il cybercrimine è ormai ovunque. Ne sentiamo parlare ogni singolo giorno. Nel 2016, oltre due miliardi di documenti sono stati persi o rubati. Nel 2017, 100 milioni di persone, soprattutto americani, hanno visto sottratti i dati della propria assicurazione sanitaria.

L'aspetto decisamente preoccupante è che, in molti casi, passano mesi prima che qualcuno segnali il furto dei documenti.

Se guardate il telegiornale la sera, penserete che gran parte di queste siano attività di spionaggio o di qualche Stato. Incredibilmente è così. Vedete, lo spionaggio è una pratica accettata a livello internazionale. Ma, in questo caso, è solo una piccola parte del problema con cui abbiamo a che fare. Quanto spesso sentite parlare di una violazione di sicurezza, seguita da "è stato il risultato di un sofisticato attacco di uno Stato?" Spesso si tratta di aziende che non vogliono assumersi responsabilità delle loro insufficienti pratiche di sicurezza.

Allora a chi è da attribuire il fenomeno? Le Nazioni Unite stimano che l'80% dei cybercrimini siano da attribuire a organizzazioni criminali altamente organizzate e sofisticate.

Ad oggi, il fenomeno rappresenta una delle economie illegali più grandi al mondo, con un fatturato di ben 445 miliardi di dollari. Fatemi mettere il numero in prospettiva: 445 miliardi di dollari è una cifra superiore al PIL di 160 nazioni, tra cui Irlanda, Finlandia, Danimarca e Portogallo, giusto per fare qualche nome e per darvi bene l'idea di cosa stiamo palando.

Ma come funziona? Come operano questi criminali?

Vi racconto una storia. Circa un anno fa, i nostri esperti di sicurezza erano sulle tracce di un trojan bancario abbastanza comune ma sofisticato, chiamato Dyre Wolf. Il Dyre Wolf si insedia nel vostro computer dopo che avete cliccato su un link di un'email civetta su cui probabilmente non avreste dovuto cliccare. Poi si siede e aspetta. Aspetta finché non entrate nel vostro conto corrente. Quando lo fate, i cattivi si intrufolano, rubano le vostre credenziali, e le usano per rubare i vostri soldi. Sembra terribile, ma la realtà è che nell'industria della sicurezza, questo tipo di attacco è quasi all'ordine del giorno.

Tuttavia, il Dyre Wolf esibiva due personalità molto diverse: una per le piccole transazioni, un'altra, completamente diversa, in caso muoveste grandi quantità di denaro tramite bonifici bancari.

Ecco cosa sarebbe successo: iniziavate il processo di emissione di un bonifico bancario, e sul vostro browser appariva una schermata della banca, che vi informava di un problema con il vostro conto e vi invitava a chiamare la banca immediatamente, indicandovi il numero del reparto frodi della banca. Quindi prendevate il telefono e chiamavate. Dopo essere passati oltre le solite indicazioni vocali, vi rispondeva un operatore in inglese. "Buongiorno, come posso esserle utile?" Così seguivate il solito processo di quando chiamate la vostra banca, fornendo il vostro nome e numero di conto, superando i controlli di sicurezza per verificare che siete chi dite di essere.

Molti di noi potrebbero non saperlo, ma per molti bonifici di importi elevati, ci vogliono due persone per approvare il trasferimento, quindi l'operatore vi chiedeva di parlare con la seconda persona, che era sottoposta alle stesse verifiche e controlli.

Sembra normale, no? C'è solo un problema: non stavate parlando con la banca. Stavate parlando con i criminali. Avevano

costruito un centralino in lingua inglese, pagine false sovrapposte al sito della banca. Era tutto eseguito in maniera così perfetta che, per ogni tentativo, muovevano da mezzo milione a un milione e mezzo di dollari nelle loro casse criminali.

Queste organizzazioni operano come vere aziende, sono sottoposte a rigida disciplina. I loro dipendenti lavorano dal lunedì al venerdì, otto ore al giorno e hanno dei turni. Sono liberi il fine settimana. Come facciamo a saperlo? Lo sappiamo perché i nostri esperti di sicurezza rilevano picchi ripetuti di malware il venerdì pomeriggio. I cattivi, dopo un lungo weekend con moglie e figli, tornano per vedere come sono andate le cose.

Passano del tempo sul Dark Web. È un termine utilizzato per descrivere il lato oscuro e senza volto di Internet, dove i ladri possono operare in anonimato senza essere scoperti. Qui smerciano i loro software di attacco e condividono informazioni su nuove tecniche di intrusione. Lì potete comprare di tutto, da software di livello base a versioni molto più avanzate. In molti casi, potete persino scegliere tra diversi livelli di servizio, oro, argento e bronzo. Potete verificare le referenze. Potete persino comprare software in garanzia "soddisfatti o rimborsati", per cautelarvi in caso di insuccesso.

Questi luoghi, questi mercati, somigliano ad Amazon o eBay. Espongono prodotti, prezzi, valutazioni e recensioni. Ovviamente, se state per comprare un attacco, lo farete da un criminale rispettabile con ottime recensioni, no?

Non è per niente diverso dal controllare Yelp o TripAdvisor prima di andare in un nuovo ristorante. Ecco un esempio. Questo è uno screenshot reale di un venditore di malware.

Notate come sia un venditore di quarta fascia, con un livello

di fiducia di sei. Lo scorso anno, ha ricevuto oltre 400 recensioni positive, solo due sono negative nello scorso mese. Ci sono addirittura dei termini di licenza.

Ecco un esempio di sito che potete visitare se volete cambiare la vostra identità.

Vi venderanno carte di identità e passaporti falsi. Notate i termini legalmente vincolanti per l'acquisto di documenti falsi. Cosa potrebbero fare, denunciarvi se li violate?

Questo è successo un paio di mesi fa: uno dei nostri esperti di sicurezza stava esaminando un nuovo malware Android che avevamo scoperto. Si chiamava Bilal Bot. In un post sul nostro blog, descrisse Bilal Bot come un'alternativa nuova, economica e in versione beta di un GM Bot molto più avanzato, diffuso nel movimento criminale. Bene, questa recensione non piacque agli autori di Bilal Bot. Quindi le scrissero una email, a difesa del loro operato, argomentando che la nostra esperta aveva valutato una versione antiquata. Le chiesero per favore di aggiornare il suo blog con informazioni più accurate e offrirono persino un'intervista per spiegarle nel dettaglio come il loro software di attacco fosse di gran lunga migliore della concorrenza.

Ecco la mail.

Attenzione, notate la natura imprenditoriale dei loro sforzi. Sembrano una vera e propria azienda.

Ma arriviamo al punto. Come facciamo a fermare questo fenomeno?

Non possiamo, per ora, identificare i responsabili. Ricordate, operano sotto anonimato e fuori dalla portata della legge. Sicuramente non riusciremmo a perseguire i criminali.

Suggerirei che abbiamo bisogno di un approccio completamente nuovo. Questo approccio deve essere basato sull'idea che dobbiamo cambiare l'economia dei cattivi.

Per darvi un'idea di come può funzionare, pensiamo alla reazione di fronte a una pandemia sanitaria: SARS, Ebola, influenza aviaria, Zika. Qual è la priorità assoluta? Localizzare chi è infetto e capire come si diffonde l'epidemia. Governi, istituzioni private, ospedali, ricercatori, rispondono tutti apertamente e rapidamente. Si tratta di uno sforzo collettivo e altruistico per fermare sul nascere la diffusione dell'epidemia e per informare ogni persona sana su come proteggersi o vaccinarsi.

Sfortunatamente, niente di questo accade di fronte a un attacco informatico. È molto più probabile che le società tengano segrete le informazioni sull'attacco. Perché? Perché fanno una pessima figura, perché hanno paura di avvantaggiare la concorrenza, di controversie legali, di regolamentazioni. Dobbiamo democratizzare in modo efficace l'intelligence sulle minacce informatiche. Bisogna che tutte le organizzazioni si aprano e condividano il contenuto del loro arsenale privato di informazioni. I cattivi si muovono rapidamente, noi dobbiamo essere più veloci di loro. Il miglior modo per farlo è quello di aprirsi e condividere dati su quello che sta succedendo.

Inculchiamo questa idea nei professionisti della sicurezza. Ricordate, il loro DNA è programmato per mantenere segreti. Dobbiamo capovolgere questa linea di pensiero. Dobbiamo fare in modo che governi, istituzioni private e aziende di sicurezza condividano informazioni velocemente. Se condividiamo le informazioni,è come se ci vaccinassimo. Se non condividiamo, siamo effettivamente parte del problema, perché aumentiamo le possibilità che altre persone possano essere colpite dalle stesse tecniche di attacco.

Bene, nel 2015 abbiamo preso una decisione drastica. Abbiamo reso il nostro database di intelligence sulle minacce (uno dei più grandi) pubblico.

Abbiamo fatto qualcosa di mai visto nel settore della sicurezza. Abbiamo iniziato a pubblicare. Oltre 700 terabyte di dati operativi sulle minacce informatiche, incluse informazioni su attacchi in tempo reale, utilizzabili per fermare il cybercrimine sul nascere. Ad oggi, oltre 4000 organizzazioni fanno leva su questi dati, tra cui metà delle aziende nella classifica Fortune 100.

La nostra speranza è di convincere tutte queste società ad unirsi a noi, fare la stessa cosa e condividere le loro informazioni su quando e come vengono attaccate. Abbiamo tutti la possibilità di fermare il cybercrimine e sappiamo già come.

*Tradotto da Francesco Truzzi*

*Revisione di Dario Mazziotta*