PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4412 di Venerdì 22 febbraio 2019

I truffatori cibernetici sono sempre più abili

Tanto si evolvono le tecniche di protezione dai truffatori informatici, tanto più abili diventano i truffatori stessi. Ecco le ultime novità nel settore.

Chi scrive si occupa di sicurezza da più di 50 anni: durante i miei corsi non manco mai di sottolineare che ho imparato molto di più dai malviventi, circa le tecniche di attacco e difesa, che non dai miei colleghi!

Non posso che confermare questa constatazione, dopo aver esaminato le ultime tecniche utilizzate dai truffatori informatici per catturare dati personali di soggetti a rischio.

Nel dicembre 2018, degli hacker, che sono stati poi ricondotti ad un sito che si trova nella Corea del Nord, hanno pubblicato su LinkedIn una ricerca di personale, diretta a professionisti informatici operanti nel settore delle banche. Parecchi professionisti del settore hanno risposto e sono stati persuasi a compilare un modulo per la richiesta di impiego, che conteneva del malware. I malviventi hanno così potuto acquisire dati personali che hanno portato alla perpetrazione di una truffa in danno di questi poveri cristi, che cercavano solo un impiego migliore.

Un'altra tecnica assai raffinata consiste nell'inviare a soggetti, presi a bersaglio, un nuovo piano di evacuazione del loro ambiente di lavoro. Scaricando il nuovo piano di evacuazione, si scarica del malware. Al contempo, sono stati inviati dei messaggi che raccomandavano di cambiare la parola chiave, sulla base delle violazioni ampiamente pubblicizzate dai mezzi di comunicazione di massa, come ad esempio la violazione che ha permesso di acquisire innumerevoli dati personali di ospiti della catena di alberghi Mariott.

Un recente studio dell'FBI ha messo in evidenza anche quale rapporto vi sia fra l'età degli obiettivi dei truffatori e i tentativi di attacco.

I soggetti con più di sessant'anni sono stati presi a bersaglio assai più spesso, rispetto ai giovani ventenni. Probabilmente il motivo non è dovuto tanto alla maggiore o minore competenza informatica dei bersagli, quanto al fatto che persone di una certa età possono avere una disponibilità economica superiore, rispetto ad un giovanotto.

La perdita media subita da giovani sotto i vent'anni si aggira sui 20 $, mentre la perdita media di un soggetto superiore a vent'anni è di poco inferiore ai 350 $.

Lo studio dello FBI è particolarmente interessante, perché mette in evidenza anche un altro accorgimento, che permette ai truffatori informatici di selezionare i bersagli. Essi accedono ai catasti urbani e cercano di identificare i soggetti che dispongono di una abitazione di vacanza, oltre all'abitazione normale. Contando sul fatto che il proprietario dell'abitazione di vacanza ha minori rapporti e minori conoscenze con l'ambiente in cui si trova l'abitazione di vacanza, essi mandano dei messaggi mirati, che segnalano ad esempio un aumento degli attacchi criminosi nella zona, raccomandando di prendere contatto con le autorità di polizia locali, per ulteriori informazioni. Ovviamente il sito Web indicato è contraffatto e i malviventi possono estrarre preziose informazioni.

Infine, una ulteriore tecnica di attacco, che sfrutta proprio la maggiore sensibilità alla sicurezza, che oggi dimostrano gli utenti del Web, fa riferimento all'utilizzo di siti Web con protezione HTTPS. Questi siti Web, contrassegnati da un lucchetto, proteggono la comunicazione fra il sito e l'utente, grazie ad un certificato SSL ? secure socket layer. La presenza di un lucchetto conferma il maggior livello di protezione nel collegamento con questi siti. Proprio per questa ragione, l'azienda GoDaddy.com, che può aprire siti Web in tempi brevi, dotati della protezione SSL, è stata indicata al pubblico come l'azienda che ha creato il maggior numero di domini phising nel primo quadrimestre del 2018, secondo la Anti Working grup ? APWG.

Chiudo questo messaggio elencando le tecniche principali di violazione utilizzate dagli hacker:

- alert per il reset della parola chiave,
- piano di evacuazione dell'edificio aggiornato,
- miglioramenti apportati alla rete di posta elettronica aziendale,
- miglioramenti apportati alla security di siti di shopping on-line,

Queste tecniche di attacco coprono quasi il 100% delle varie tecniche utilizzate.

Adalberto Biasiotti

www.puntosicuro.it