PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5764 di Venerdì 10 gennaio 2025

RAT: un efficace strumento di contrasto del crimine informatico via Internet

L'FBI ha pubblicato un rapporto sui crimini informatici, perpetrati via Internet che mette in evidenza l'efficienza ed efficacia di una struttura di pronto intervento, chiamata RAT ? Recovery Asset Team, che contrasta le BEC - Business Email Compromise.

Come tutti gli anni, lo FBI ha pubblicato un rapporto sui crimini informatici, perpetrati via Internet. La lettura del rapporto è oltremodo illuminante, anche perché mette in evidenza l'efficienza ed efficacia di una struttura di pronto intervento, chiamata RAT ? Recovery Asset Team, che contrasta le BEC - Business Email Compromise.

I lettori vorranno perdonarmi se ho utilizzato, in poche righe, due acronimi, la cui importanza è tuttavia fondamentale per classificare gli attacchi informatici via Internet ed attivare procedure di tempestivo intervento su tentativi di frode.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[ALDIG02] ?#>

Questi aspetti vengono ampiamente illustrati nel rapporto sui crimini perpetrati via Internet, che i lettori trovano in allegato, che illustra le tre aree principali, nelle quali vengono scomposti questi specifici tipi di crimine:

- il crimine viene perpetrato perlopiù grazie ad una BEC- Business Email Compromise. Grazie a questo attacco, il bersaglio riceve un messaggio di posta elettronica, che ha tutte le apparenze di credibilità, e viene indotto, ad esempio, ad effettuare versamenti su conti correnti, in capo ai malviventi,
- la vittima deve inviare con urgenza un messaggio di allarme allo IC3-Internet Crime Complaint Center. Si tratta di una struttura specialmente costruita dallo FBI, che raccoglie non solo elementi di tipo statistico, ma anche elementi necessari per attivare un rapido strumento di blocco della transazione fraudolenta,
- infine, l'informazione sulla transazione fraudolenta viene inviata al RAT - Recovery Asset Team, che è in grado di prendere immediato contatto con le istituzioni finanziarie coinvolte e provvedere al blocco della transazione fraudolenta.

L'efficienza ed efficacia di questa struttura evidentemente è condizionata dal fatto che la vittima invii al più presto possibile le informazioni circa la frode di cui ritiene di essere rimasta vittima; successivamente le due strutture provvedono ad un rapidissimo scambio di informazioni, con l'attivazione dei contatti con le istituzioni finanziarie coinvolte. Nel testo di questo rapporto, di cui raccomandiamo caldamente la lettura ai lettori, sono citati alcuni esempi, legati agli esiti positivi e al blocco tempestivo della transazione fraudolenta.

Il rapporto è arricchito da tutt'una serie di dati statistici, che illustrano gli importi coinvolti, la frequenza delle transazioni e soprattutto le tipologie di attacco, più frequentemente utilizzate dai malviventi. Si tratta di una lettura oltremodo educativa, anche perché, mettendo a confronto annate diverse, è possibile osservare l'evoluzione degli strumenti di attacco, da parte dei malviventi informatici.

Un aspetto che viene messo in evidenza riguarda anche un picco di schemi di investimento in cripto valute, che hanno natura fraudolenta.

Anche il ransomware è in costante aumento, e lo FBI ha identificato almeno cinque diverse tipologie di attacco, che riguardano in particolare le infrastrutture critiche.

Anche questa indagine mette in evidenza come particolarmente esposti agli attacchi siano i soggetti in età avanzata, sia in termini di numero di soggetti attaccati, sia in termini di perdite subite.

Un'interessante tabella è illustrata a pagina 18, laddove vengono messe a confronto le situazioni riscontrate in 20 paesi del mondo, ivi compresa l'Italia.

Il documento è completato da un glossario, che risulta oltremodo utile per consentire a soggetti, distribuiti in varie parti del mondo, di adottare riferimenti uniformi, che permettano di effettuare con rapidità ed affidabilità il confronto fra le situazioni che si incontrano in vari contesti.

Infine, l'appendice C del rapporto offre preziosi link di collegamento a documenti similari, sviluppati in varie parti del mondo. Questo ricchissimo materiale di supporto permette di allargare ed approfondire l'indagine di una tipologia di reato, che purtroppo potrà solo aumentare nel tempo.

Internet Crime Complaint Center - Federal Bureau of Investigation - Internet Crime Report 2023.

Adalberto Biasiotti

Licenza Creative Commons
I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.