L’FBI smantella la botnet Qakbot. Sequestrati 8,6 milioni di dollari in criptovaluta

Addio ad una della più grandi *botnet malware* attive nel panorama internazionale, responsabile di danni per “centinaia di milioni” di dollari a livello globale.

Ieri, l’FBI ha annunciato di aver “interrotto e smantellato” con successo il malware **Qakbot**, identificando oltre 700.000 computer infetti in tutto il mondo, di cui più di 200.000 negli Stati Uniti. Il Dipartimento di Giustizia ha inoltre annunciato il sequestro di oltre 8,6 milioni di dollari in criptovaluta dall’organizzazione cybercriminale di Qakbot, somma che sarà ora resa disponibile alle vittime.

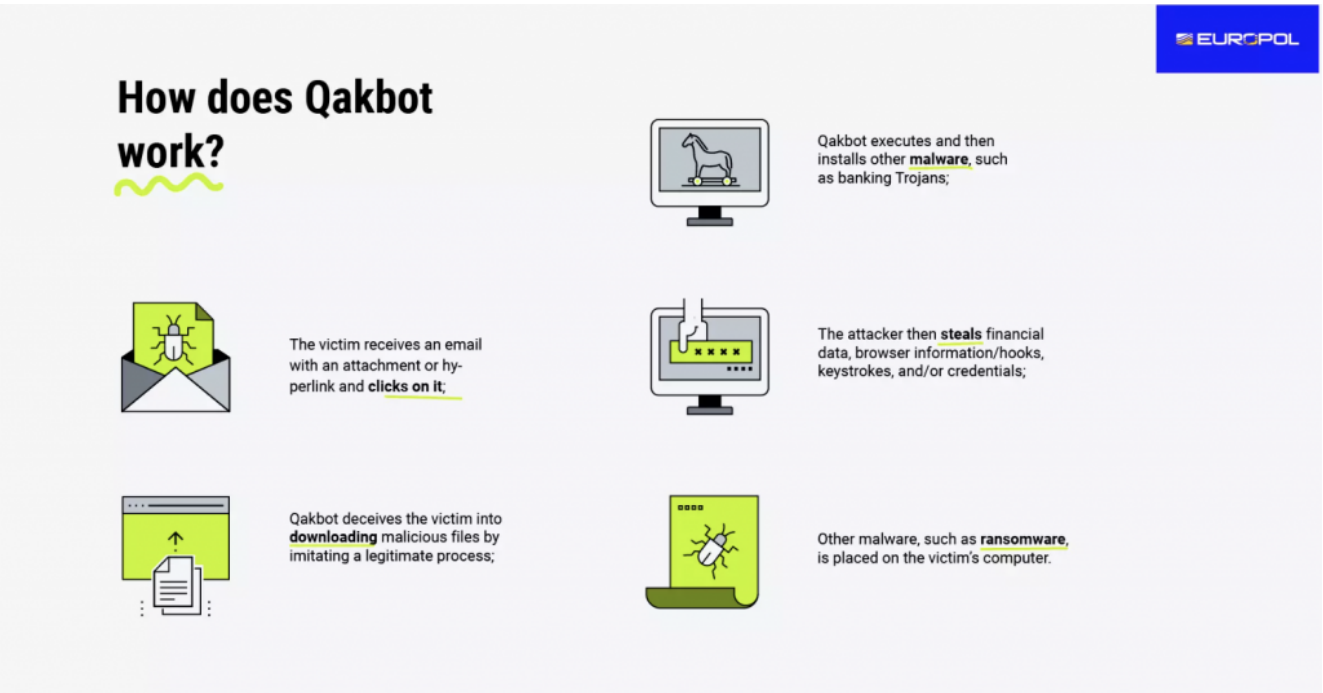
“L’FBI ha neutralizzato questa catena di approvvigionamento criminale di vasta portata, tagliandola alle radici”, ha dichiarato il Direttore dell’FBI **Christopher Wray** in un videomessaggio. *“Le vittime andavano dalle istituzioni finanziarie sulla costa orientale a un contraente governativo per infrastrutture critiche nel Midwest, fino a un produttore di dispositivi medici sulla costa occidentale.”*

[embedded content]
L’operazione, condotta in collaborazione con le forze dell’ordine di Francia, Germania, Paesi Bassi, Romania, Lettonia e Regno Unito, rappresenta la più grande interruzione finanziaria e tecnica di un’infrastruttura botnet guidata dagli Stati Uniti, utilizzata dai cybercriminali per commettere ransomware, frodi finanziarie e altre attività criminali online.

Come funzionava il malware Qakbot

Il malware Qakbot è stato utilizzato per infettare i computer delle vittime tramite messaggi e-mail di spam contenenti allegati dannosi, ha affermato il Dipartimento di Giustizia. Una volta cliccato e attivato, l'agente malevolo agiva installando un ransomware, spegnendo i computer delle vittime e portando i criminali a richiedere il pagamento di un riscatto per sbloccare i dispositivi, ha affermato il dipartimento.

Una volta che le autorità hanno ottenuto l'accesso all'infrastruttura Qakbot è stato possibile identificare più di 700.000 computer in tutto il mondo, di cui 200.000 nei soli Stati Uniti, infettati dal malware. Sin dalla sua creazione nel 2008, il malware Qakbot è stato utilizzato in attacchi di ransomware e in altri reati informatici che hanno causato danni per centinaia di milioni di dollari a individui e aziende negli Stati Uniti e all'estero.



"Questa botnet ha fornito a criminali informatici come questi un'infrastruttura di comando e controllo composta da centinaia di migliaia di computer utilizzati per attacchi contro individui e aziende in tutto il mondo", ha dichiarato Wray.

“Tutto questo è stato reso possibile dal lavoro dedicato dell’FBI di Los Angeles, dalla nostra Divisione Cyber presso la sede dell’FBI e dai nostri partner, sia qui che all’estero”, ha affermato Wray. *“La minaccia informatica che affronta la nostra nazione sta diventando ogni giorno più pericolosa e complessa. Ma il nostro successo dimostra che la nostra stessa rete e le nostre stesse capacità sono più potenti.”*

https://www.key4biz.it/lfbi-smantella-la-botnet-qakbot-sequestrati-86-milioni-di-dollari-in-criptovaluta/457551/