Affitto l'hacker per bloccare il sito del rivale

CAROLA FREDIANI

«Sto cercando un servizio a pagamento per mandare offline un sito per più tempo possibile, tre volte a settimana». Così scrive un utente sul sito Hackforums, molto frequentato da ragazzini. Ma, evidentemente, anche da chi voglia regolare dei conti. Per vendetta personale, tornaconto, concorrenza sleale. Abbondano, qui e su molti altri siti di hacking, inserzioni di chi cerca e offre attacchi informatici.

CONTINUA A PAGINA 15

Inchiesta

CAROLA FREDIANI

SEGUE DALLA PRIMA PAGINA

Un mercato che esiste da tempo, ma ora una serie di fattori lo stanno rendendo più preoccupante. Non ultimo l'episodio di qualche giorno fa che ha reso irraggiungibili per ore una serie di siti di primo piano, da Twitter a Spotify. Il fornitore di servizi internet di quei siti è stato ingolfato dalle richieste di accesso di una miriade di dispositivi sparsi per il mondo. Sono botnet, reti di computer - e non solo, come vedremo - infettati e controllati da remoto. Negli ultimi anni si è sempre più sviluppato un florido mercato di botnet a noleggio. O, se volete, di Ddos in affitto, dove Ddos (Distributed Denial of Service) indica proprio quel tipo di attacco distribuito che, tempestando di richieste (pacchetti) un sito, lo rende irraggiungibile.

Un annuncio che abbiamo trovato su AlphaBay, un noto mercato nero underground, pubblicizza un servizio di Ddos in affitto che dispone di 25mila sistemi compromessi distribuiti su un centinaio di Paesi. Comprare un attacco che mandi offline un sito per 24 ore, dice l'inserzione, può costare fino a 400 euro. Ma anche di meno, a seconda del target e di quanto abbia le spalle larghe.

«I miei prezzi variano da pochi dollari fino a 500 all'ora», mi dice un venditore di Ddos che ho raggiunto in una chat cifrata dopo aver trovato le sue inserzioni. «Posso attaccare siti di gaming, casinò online, ma anche aziende di media grandezza». La sua botnet è composta da computer Windows infettati. «Il business delle botnet va a gonfie vele e il settore dove ci sono più soldi è quello indirizzato al settore finanziario. Botnet usate per rubare dati e credenziali bancarie. La mia la uso solo per rivendere Ddos: è un'attività che esiste da tempo, ma sta progressivamente crescendo».

Sempre su Hackforums invece si trova la pubblicità di un negozio online, grafica scintillante, che vende direttamente bot, cioè computer infettati, come fossero patate, un tanto al chilo: 0,04 dollari a bot, 0,08 se si vuole anche gli aggiornamenti. Se ne possono comprare in blocco fino a 6mila.

In pratica è un mercato che offre servizi a livelli diversi. «Puoi comprarti gli strumenti, cioè il software per costruirti una botnet tu stesso. Oppure, puoi comprarne una chiavi in mano, fatta da altri. O infine, puoi comprare direttamente solo degli attacchi pagati a ore», commenta a La Stampa Antonio Forzieri, esperto di sicurezza di Symantec.

Come rilevato da ricercatori di Rsa e F-Secure, all'inizio di ottobre era pubblicizzata online una botnet molto ampia di vari apparecchi connessi a internet: 7500 dollari per avere a disposizione ben 100mila dispositivi, molti dei quali non erano neppure pc.

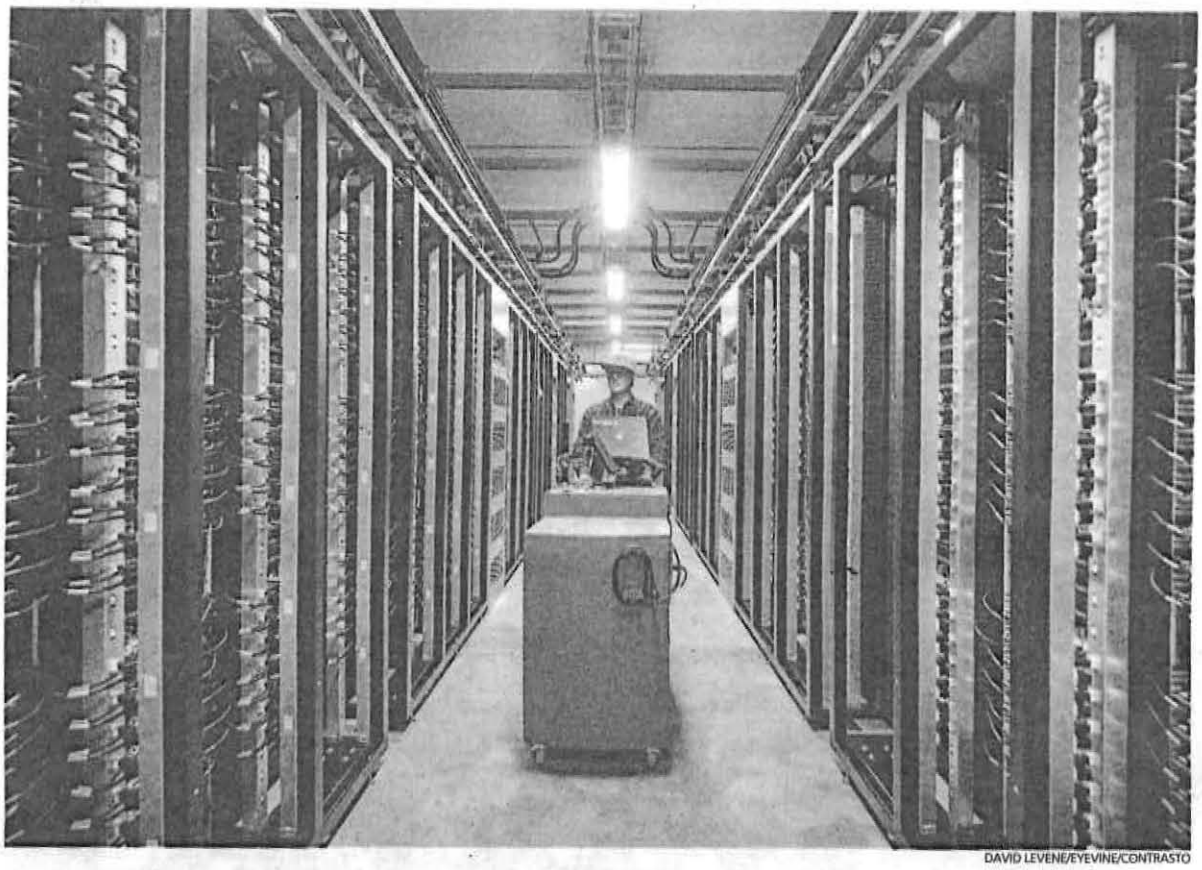
Ed è proprio questa una delle novità del settore. La diffusione di botnet che sempre di più sfruttano la cosiddetta internet delle cose: router, videoregistratori, videocamere soprattutto, e in prospettiva anche frighi, tv, tostapane intelligenti. Ovvero connessi in Rete. Come la botnet Mirai, ormai divenuta famosa. È composta da circa 120mila dispositivi di questo genere, specie videocamere e videoregistratori, in parte prodotti da una stessa azienda cinese, Xiongmai. Dispositivi che hanno una serie di password predeterminate che non verranno mai cambiate: per cui si deve solo provarle, accedere, prendere il controllo. Questa botnet Mirai è stata usata a metà settembre per bombardare il sito di un giornalista, Brian Krebs. Quindi il suo codice è stato pubblicato su un forum a fine settembre, forse per depistare e scansare l'attenzione delle forze dell'ordine. Il risultato? «Dal rilascio del suo codice, si sono diffuse diverse botnet simili. Insomma, ora ci sono più Mirai, non più solo una. Un paio di queste vendono attacchi. E una parte è stata coinvolta nell'aggressione che ha travolto Twitter, Spotify, PayPal», commenta a La Stampa il ricercatore noto online come @2sec4u che ha investigato Mirai insieme all'azienda Malwaretech. «Mi aspetto di vedere nuove botnet spuntare da qui a breve». E ulteriori attacchi.

Ultimi casi

Bbc
A gennaio scorso contro il sito giornalistico è stato portato un attacco Ddos di oltre 600 Gigabite per secondo

Ovh
A settembre viene colpita l'azienda di hosting con un attacco di un Terabit per secondo

Dyn
Di recente è stato colpito il fornitore di servizi internet e Dns colpendo indirettamente colossi come Twitter, Spotify e Paypal



DAVID LEVENE/EYEVINE/CONTRASTO

Bloccare un sito è facile Ora basta affittare un attacco pagando a ore

Vendetta personale o concorrenza sleale non importa Costa 400 dollari oscurare qualcuno per un giorno intero

Datacenter
Spesso gli attacchi attraverso le botnet colpiscono grossi datacenter