

IoT botnet, al Black Hat si studia la nuova cyber minaccia per le reti energetiche globali

Le **botnet** sono ormai considerate tra le minacce più rilevanti ai sistemi di sicurezza informatici di imprese e organizzazioni pubbliche. Si tratta di una rete di *robot* (quindi anche *software* oltre che *hardware*) controllata da remoto da *botmaster* per compiere cyber attacchi

Affinchè una botnet sia efficace per un attacco informatico deve essere di grandi dimensioni. Più è grande il numero di device “*zombie*” controllati da remoto, più grande è il danno che sono in grado di arrecare.

La minaccia delle IoT botnet

Per capire come lavora una botnet basta prendere ad esempio il celebre caso “*Mariposa*” del 2010: una rete di computer zombie che ha infettato almeno 13 milioni di pc in 190 Paesi, inclusi numerosi pc di grandi aziende (oltre la metà delle 1.000 aziende più grandi al mondo) e almeno 40 importanti banche.

Alla conferenza **Black Hat** sezione americana è stato presentato uno studio dedicato all’impiego di **botnet dell’*Internet of Things*** (IoT) nel settore della generazione e distribuzione dell’energia elettrica.

IoT botnet non solo in grado di influenzare il funzionamento

delle reti energetiche, ma di condizionare anche il mercato di riferimento.

Parliamo di device connessi in rete di ogni tipo, dalle apparecchiature più sofisticate per la gestione dei flussi delle risorse energetiche ai più semplici *smart meter* (contatori) in dotazione ormai di ogni famiglia.

La domanda da porsi è la seguente, secondo i ricercatori: *“In che modo i cyber criminali utilizzeranno questa botnet IoT? Con quale intensità? Per causare danni o per fare profitti? O per raggiungere entrambi gli obiettivi?”*.

Oggi basta una IoT botnet di 50 mila device connessi in rete e tra loro per causare danni ad imprese ed enti pubblici, quindi danni ai cittadini., secondo i ricercatori del Georgia Institute of Technology (Git).

Facili guadagni o danni sempre più grandi?

Tramite uno strumento del genere sarebbe possibile causare un **blackout energetico** in una città o in alcuni dei suoi quartieri, oppure **sottrarre energia elettrica** a migliaia di ignari cittadini senza che questi se ne accorgano, o **manipolare gli scambi di domanda-offerta sul mercato americano**, senza che nessuno se ne renda conto.

Questo tipo di azione comporterebbe un aumento dei costi in bolletta del 7% circa, un dato molto contenuto di cui in pochi si accorgerebbero su decine di milioni di utenti.

Al contrario, per i cyber criminali i guadagni sono altissimi: considerando il caso di un attacco effettuato per tre ore al giorno, per un periodo di tempo di 100 giorni in un anno, il bottino potrebbe essere di circa 24 milioni di dollari all'anno, mentre con lo stesso sistema si potrebbero anche

infliggere perdite per 350 milioni di dollari l'anno.

Per questo i ricercatori suggeriscono, ad esempio, di porre maggiore attenzione agli smart device ad alto voltaggio, perché sono quelli più utilizzati nelle reti IoT impiegate nel settore energetico.

Cosa fare?

Solo casi ipotetici, purtroppo no.

Negli Stati Uniti, la Commissione federale di regolamentazione dell'energia ha indagato su 16 potenziali casi di manipolazione del mercato nel 2018, sebbene ne abbia chiusi 14 senza provvedimenti.

Inoltre, a metà maggio di quest'anno, un cyber attacco di vasta portata ha violato i sistemi IT di Elexon, la piattaforma informatica utilizzata per gestire il mercato energetico del Regno Unito.

Molto utili, a riguardo, potrebbero essere sistemi di monitoraggio in tempo reale, in grado di segnalare anche la più piccola variazione nei flussi, nei consumi e negli scostamenti di domanda e offerta.

Per anticipare le mosse dei cyber criminali odierni bisogna pensare in maniera diversa, magari iniziando ad immaginare l'impensabile. Come ha spiegato su wired.com, il fondatore di Fortiphyd Logic: *"Chi avrebbe mai detto che i nuovi attacchi informatici avrebbero usato come porta principale la mia lavatrice connessa in rete o il frigorifero smart?"*.

<https://www.key4biz.it/iot-botnet-al-black-hat-si-studia-la-nuova-cyber-minaccia-per-le-reti-energetiche-globali/317629/>