

Emotet: Il CERT-AGID avverte del ritorno del trojan



A pochi mesi dall'ultima campagna rilevata (risalente allo scorso 15 luglio), oggi una nota diffusa dal Computer Emergency Response Team dell'AGID – Agenzia per l'Italia Digitale informa di aver notato una recrudescenza negli attacchi veicolati dalla botnet Emotet e diretti contro target italiani.

Sul fronte degli attaccanti, la distribuzione dei server *Command and Control* da cui è stata lanciata la campagna di *phishing* non porterebbe a collocarne nessuno in Italia; i 58 C2 osservati – riconducibili a IP già usati nella botnet Emotet denominata Epoch4 – appaiono infatti sparsi fra Nord Europa, Stati Uniti, Brasile, Sudafrica e Sud-Est asiatico.

Anche le tecniche utilizzate sarebbero pressoché identiche a quelle impiegate nei casi precedenti: secondo la nota diffusa dal CERT, gli attacchi continuano a “veicolare tramite email un allegato ZIP protetto da password e contenente un XLS dotato di macro malevola”, mirando “al download della solita DLL (64bit) Emotet che viene eseguita utilizzando il classico comando *regsvr32*”.

A beneficio di utenti e organizzazioni, è già stata pubblicata una lista di indicatori di compromissione (IoC) utili a identificare l'eventuale presenza del malware entro il perimetro dei propri sistemi.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/emotet-il-cert-agid-avverte-del-ritorno-del-trojan/>