Emotet, il banking trojan è tornato. Come proteggersi

Dopo una pausa di ben cinque mesi Emotet torna a far parlare di sè con una nuova e massiccia campagna **malspam** rilevata venerdì 17 luglio scorso e che sta interessando vari paesi nel mondo tra cui l'Italia.

Il trojan bancario Emotet, apparso in natura per la prima volta nel 2014, si è nel tempo evoluto fino a diventare un vero e proprio framework criminale multi funzione. Prima della sua temporanea scomparsa, presentandosi in diverse forme ha rappresentato di sicuro una delle principale minacce nel 2018, nel 2019 e nei primi mesi del 2020 in pieno inizio era COVID-19.

La campagna in atto

Come segnalato anche dai ricercatori di Malwarebytes, le botnet Emotet hanno iniziato a veicolare malspam, utilizzando le consuete tecniche utilizzate già in passato. Nella fattispecie sono stati rilevati campioni e-mail, anche recapitati come risposte in contesti di comunicazioni già esistenti, contenenti allegati o link URL che fanno riferimento a file Microsoft Office malevoli.

In ogni caso il documento scaricato contiene una macro, con codice altamente offuscato, che una volta abilitata, recupera via Powershell (tramite *Windows Management Instrumentation,* WMI) il file binario Emotet dal primo server remoto disponibile ed identificato tra quelli presenti in un elenco di siti Web compromessi.

Il payload, una volta eseguito, dopo aver inviato una conferma al relativo server di comando e controllo, può attendere anche diversi giorni prima di intraprendere ulteriori azioni o installare altre forme di malware (come il trojan Trickbot e il ransomware Ryuk) sul computer della malcapitata vittima.

Come proteggersi

Poiché, come noto, uno dei moduli Emotet consente al trojan di rubare anche credenziali e-mail e quindi di diffondersi mediante messaggi infetti provenienti da utenti presenti tra i nostri contatti, per evitare di diventare noi stessi un ulteriore vettore di propagazione, è importante pensare di proteggere anche ogni nostro account, utilizzando password diverse per ogni profilo, attivando se possibile sia meccanismi di autenticazione a due fattori che l'invio di messaggi di alerting in caso di accessi anomali.

In ogni caso risultano anche utili allo scopo le raccomandazioni di protezione che solitamente si suggeriscono per contrastare il phishing:

- prestare sempre la massima cautela quando si ricevono e-mail di provenienza sospetta o da mittenti sconosciuti;
- evitare di aprire allegati e di abilitare l'esecuzione di macro Microsoft Office, anche se apparentemente legittime.

Di seguito gli IoC relativi alla campagna in corso e pubblicati dai ricercatori Mawarebytes.

Hash dei documenti malevoli

5d2c6110f2ea87a6b7fe9256affbac0eebdeee18081d59e05df4b4a17417492b
4fdff0ebd50d37a32eb5c3a1b2009cb9764e679d8ee95ca7551815b7e8406206
bb5602ea74258ccad36d28f6a5315d07fbeb442a02d0c91b39ca6ba0a0fe71

a2
6d86e68c160b25d25765a4f1a2f8f1f032b2d5cb0d1f39d1d504eeaa69492d
e0
18fab1420a6a968e88909793b3d87af2e8e1e968bf7279d981276a2aa8aa67
8e
d5213404d4cc40494af138f8051b01ec3f1856b72de3e24f75aca8c024783e
89

URL dei siti compromessi

elseelektrikci [.] com
rviradeals [.] com
skenglish [.] com
packersmoversmohali [.] com
tri-virgola [.] com
ramukakaonline [.] com
shubhinfoways [.] com
test2.cxyw [.] net
sustainableandorganicgarments [.]
staging .icuskin [.] com
fivestarcleanerstx [.] com
bhandaraexpress [.] com
crm.shaayanpharma [.] com
zazabajouk [.] com
e2e-solution [.] com
topgameus [.] com
cpads [.] net
tyres2c [.] com
thesuperservice [.] com
ssuse [.] com

File binari

454d3f0170a0aa750253d4bf697f9fa21b8d93c8ca6625c935b30e4b188353
74
d51073eef56acf21e741c827b161c3925d9b45f701a9598ced41893c723ace
23

1368a26328c15b6d204aef2b7d493738c83fced23f6b49fd8575944b94bcfbf4
7814f49b3d58b0633ea0a2cb44def98673aad07bd99744ec415534606a9ef314
f04388ca778ec86e83bf41aa6bfa1b163f42e916d0fbab7e50eaadc8b47caa50

Indirizzi IP dei server di comando e controllo

178.210.171 [.] 15
109.117.53 [.] 230
212.51.142 [.] 238
190.160.53 [.] 126

https://www.key4biz.it/emotet-il-banking-trojan-e-tornato-come-proteggersi/315373/