Malware, la botnet Emotet non esiste più

Emotet, la botnet malware più grande al mondo, non esiste più. Grazie ad un'operazione internazionale coordinata dall'Europol e dall'Eurojust in collaborazione con le autorità giudiziarie di Germania, Paesi Bassi, Stati Uniti, Regno Unito, Francia, Lituania, Canada e Ucraina, uno dei servizi di criminalità informatica più professionali e duraturi in circolazione, è stato sconfitto.

Emotet: la botnet attiva dal 2014

Apparsa in natura per la prima volta nel 2014, la botnet si è evoluta nel tempo fino a diventare un vero e proprio framework criminale multi funzione. Emotet è un malware che si è diffuso nel corso degli anni passati prevalentemente tramite e-mail di phishing contenenti documenti Word infetti con un codice dannoso. Lo scopo di Emotet è quello installare una backdoor sui sistemi Windows così da renderli disponibili a vari scopi: distribuzione di ulteriore malware, ransomware e installazione di strumenti di accesso remoto.

EMOTET takedown

EUROPOL

In January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet.

Participating law enforcement authorities:

- Netherlands (Politie)
- Germany (Bundeskriminalamt)
- France (Police Nationale)
- Lithuania (Lietuvos kriminalinės policijos biuras)
- Canada (Royal Canadian Mounted Police)
- USA (Federal Bureau of Investigation)
- UK (National Crime Agency)
- Ukraine (Національна поліція України)

EUROPOL

How did Emotet work?

Luring the victims

Emotet was delivered to the victims' computers via emails that contained a malicious link or an infected document.

Installation

If victims opened the attachment or the link, the malware got installed.

Infection

The computer became vulnerable and was offered for hire to other criminals to install other types of malware.

Emotet opened doors for:

- **Information stealers**
- **Trojans**
- **Ransomware**

Trickbot, QakBot and Ryuk were among the malware families to use Emotet to enter a machine.

What made Emotet so dangerous?

Long lasting	Started as a banking Trojan in 2014, evolving over time.
Go-to-solution for criminals	It acted as a door opener for other computers, allowing unauthorised access to other malware families.
Polymorphic	It changed its code each time it was called up.
Resilient	Unique way of infecting networks by spreading the threat after gaining access to just a few devices in the network.

Protect yourself from malware

Always check your emails carefully and watch out for:

- attachments or embedded links from unknown senders.
- messages with a sense of urgency asking you to download something.
- offers with a promise of reward that sounds too good to be true.

Fonte: Europol

La collaborazione con i CSIRT

“Per interrompere l’infrastruttura Emotet, si legge nel comunicato dell’Europol, *le forze dell’ordine hanno collaborato per creare una strategia operativa efficace. Dato che l’infrastruttura utilizzata da Emotet ha coinvolto diverse centinaia di server dislocati in tutto il mondo, tutti dotati di funzionalità diverse per gestire i computer delle vittime infette, in un’operazione durata una settimana le forze dell’ordine e le autorità giudiziarie hanno acquisito il controllo dell’infrastruttura e l’hanno rimossa dall’interno. Le macchine infette delle vittime sono state reindirizzate verso questa infrastruttura controllata dalle forze dell’ordine”,* ha spiegato l’Europol. *“Un approccio nuovo e unico per interrompere efficacemente le attività dei facilitatori del crimine informatico”.*

L’Europol sta infine collaborando con i **Computer Emergency Response Team** (CSIRT) in tutto il mondo per aiutare coloro che hanno subito infezioni da parte di Emotet. L’indagine è comunque ancora in corso per l’identificazione dei responsabili e della loro gestione una volta individuati.

https://www.key4biz.it/malware-la-botnet-emotet-non-esiste-piu/341932/