ONTMANTELING BOTNET EMOTET

EUROPOL

Deelnemende landen

- Nederland (politie)
- Duitsland (Bundeskriminalamt)
- Frankrijk (Police Nationale)
- Canada (Royal Canadian Mounted)
- VS (Federal Bureau of Investigation)
- VK (National Crime Agency)
- Oekraïne (Національна поліція України)

EUROPOL

Hoe werkte Emotet?

Slachtoffers

Emotet besmette computers van slachtoffers door middel van e-mails met een link of document.

Installatie

Als de slachtoffers op de link klikten of het document openden, werd de malware geïnstalleerd.

Besmetting

De computer werd kwestbaar en door Emotet aan andere criminelen aangeboden om malware op te installeren.

Emotet opende de deuren voor

Informatie-dieven

Trojaanse paarden

Gijzelsoftware (ransomware)

Trickbot, QakBot and Ryuk waren een paar van de malware-families die gebruik maakten van Emotet.

Waarom was Emotet zo gevaarlijk?

Lang bestaan	Begon in 2014 en ontwikkelde zich sindsdien.
Go-to-oplossing voor criminelen	Fungeerde als het ware als een deuropener voor andere malware-families.
Polimorf	Veranderde steeds haar code (moeilijker te detecteren).
Veerkrachtig	Unieke manier van netwerken infecteren.

Bescherm jezelf tegen malware

Controleer je e-mails en pas op voor:

Bijlagen of hyperlinks van onbekende afzenders.

Berichten die je dringend verzoeken iets te downloaden.

Aanbiedingen die te mooi klinken om waar te zijn.