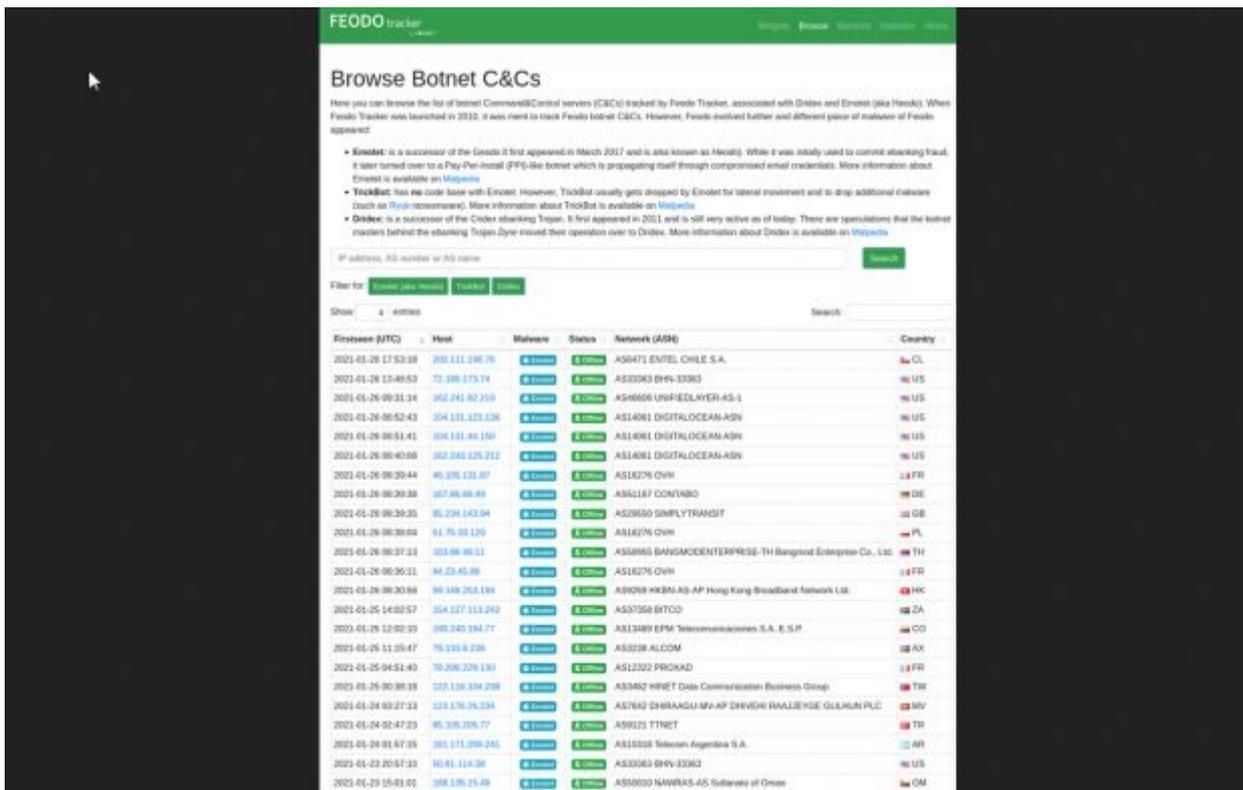


# Bye bye, Emotet



The screenshot shows the FEODO Tracker interface. At the top, it says "FEODO tracker" and "Browse Botnet C&Cs". Below this, there is a brief introduction and a list of botnets: Emotet, TrickBot, and Dridex. A search bar is present with the text "Filter for: Emotet (34 results) | TrickBot | Dridex". Below the search bar, there is a table with columns: Firstseen (UTC), Host, Malware, Status, Network (ASN), and Country. The table lists various botnet C&Cs with their first seen dates, host IP addresses, malware types, and the networks they are associated with.

Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Country
2021-01-26 17:53:38	203.121.236.76	Emotet	Active	AS6473 ENTEL CHILE S.A.	CL
2021-01-26 13:46:53	72.188.273.74	Emotet	Active	AS3363 BNY-3363	US
2021-01-26 09:31:34	362.241.92.259	Emotet	Active	AS4666 UNF-EDLAYER-AS-1	US
2021-01-26 06:52:43	204.121.123.126	Emotet	Active	AS14061 DIGITLOCEAN-ASN	US
2021-01-26 06:51:41	104.121.48.150	Emotet	Active	AS14061 DIGITLOCEAN-ASN	US
2021-01-26 06:40:68	362.240.126.212	Emotet	Active	AS14061 DIGITLOCEAN-ASN	US
2021-01-26 06:39:44	46.205.121.87	Emotet	Active	AS16276 OVH	FR
2021-01-26 06:39:35	257.86.88.49	Emotet	Active	AS61167 CONFIABO	DE
2021-01-26 06:39:35	85.234.143.94	Emotet	Active	AS25650 SIMPLYTRANSIT	DE
2021-01-26 06:39:04	51.76.83.120	Emotet	Active	AS16276 OVH	PL
2021-01-26 06:37:23	203.96.86.51	Emotet	Active	AS58865 BANGMAIDENTERPRISE-TH Bangkok Enterprise Co., Ltd	TH
2021-01-26 06:36:11	84.23.45.88	Emotet	Active	AS16276 OVH	FR
2021-01-26 06:30:59	99.148.253.191	Emotet	Active	AS8028 HKBN-AS-AP Hong Kong Broadband Network Ltd.	HK
2021-01-25 14:02:57	154.127.113.242	Emotet	Active	AS37058 BITOC	ZA
2021-01-25 12:02:33	185.240.194.77	Emotet	Active	AS13489 EPM Telefonosdelosandes S.A. E.S.P.	CO
2021-01-25 11:26:47	76.123.4.236	Emotet	Active	AS3228 ALCOM	AX
2021-01-25 04:51:43	70.204.226.130	Emotet	Active	AS12302 PROxad	FR
2021-01-25 00:38:39	123.136.324.228	Emotet	Active	AS3462 HNET Data Communication Business Group	TR
2021-01-24 03:27:13	123.176.26.134	Emotet	Active	AS7642 DHRAAGU MV-AP DNVISHI RAALIESE GULUM PLC	MY
2021-01-24 02:47:23	85.305.205.77	Emotet	Active	AS8923 TTNET	TR
2021-01-24 01:47:35	185.171.299.245	Emotet	Active	AS18328 Telecom Argentina S.A.	AR
2021-01-23 20:57:23	80.81.114.38	Emotet	Active	AS33363 BNY-3363	US
2021-01-23 15:01:02	384.136.15.49	Emotet	Active	AS5000 NAWRAS-AS Sultanate of Oman	OM

A gennaio scorso avevo [segnalato](#) che un intervento coordinato di varie forze dell'ordine in numerosi paesi aveva messo fuori uso Emotet, uno dei [malware](#) più diffusi, che da solo era responsabile di circa il 30% di tutti gli attacchi informatici.

La tecnica era classica: un documento Word, che molti utenti ritengono innocuo, conteneva il malware, che veniva lanciato se la vittima apriva il documento e attivava le [macro](#) in Microsoft Word.

Ora è arrivata la conclusione dell'intervento di polizia: il 25 aprile scorso i computer che erano stati infettati da Emotet hanno cancellato il malware. Questo è stato possibile perché le forze di polizia avevano preso il controllo degli aggiornamenti di Emotet e ne avevano diffuso uno autodistruttivo.

Alla scadenza impostata, appunto il 25 aprile, è scattata l'autodistruzione. Il [portale dedicato ad Emotet](#) presso

Abuse.ch indica ora zero computer infetti, che è un risultato notevolissimo, considerato che Emotet aveva preso il controllo di oltre un milione di computer in tutto il mondo, generando incassi illegali per oltre 2 miliardi di dollari.

Va [notato](#) che in un intervento come questo le forze di polizia in sostanza aggiornano forzatamente i computer infettati, senza chiedere il consenso dei rispettivi proprietari, ponendo interrogativi sulla legalità di questa tecnica, indubbiamente efficace ma potenzialmente pericolosa. Ovviamente in questo caso nessun protesta, però è formalmente un'intrusione.

Anche l'FBI di recente ha [usato](#) lo stesso approccio per ripulire a forza i server Microsoft Exchange infettati da una serie di attacchi denominati *Hafnium*, visto che i legittimi proprietari di questi server si ostinavano a non aggiornarli.