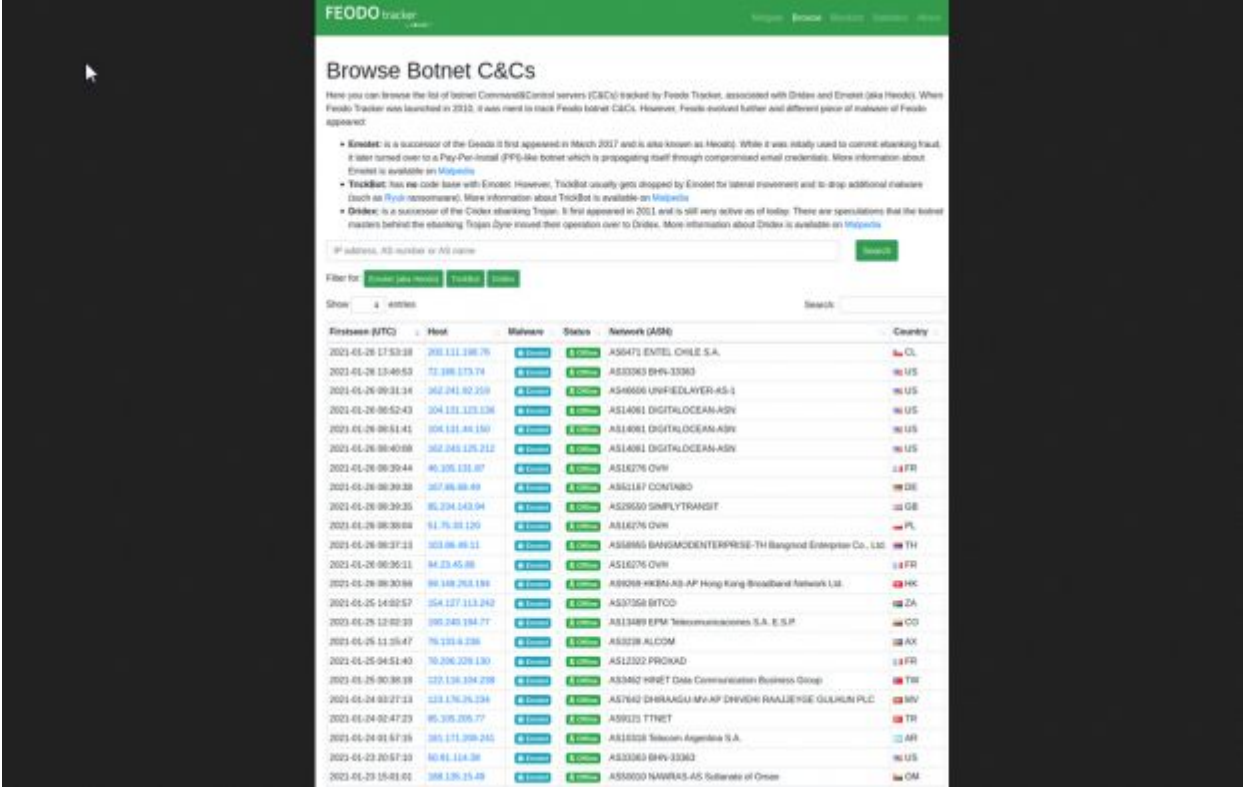

Tempo di lettura: 50 sec

Autore: Paolo Attivissimo

<https://www.zeusnews.it/n.php?c=28756>

Bye bye, Emotet

CREATORIdiFUTURO.it



The screenshot shows the FEODO Tracker interface. At the top, there's a green header with the logo and navigation links. Below it, a section titled 'Browse Botnet C&Cs' provides context about the tracker and lists botnets like Emotet, TrickBot, and Oxybot. A search bar is present. The main part of the page is a table with columns: Firstseen (UTC), Host, Malware, Status, Network (ASN), and Country. The table lists various botnet command and control servers with their first seen dates, host IP addresses, associated malware, status (active/inactive), the network they belong to (ASN), and their geographical location (country).

Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Country
2021-01-26 17:53:38	203.111.198.76	Emotet	Active	AS6471 ENTEL CHILE S.A.	CL
2021-01-26 13:49:53	72.186.173.74	Emotet	Active	AS33063 BNY-33063	US
2021-01-26 09:31:34	162.241.82.259	Emotet	Active	AS46666 UNIFIEDLAYER-AS-1	US
2021-01-26 06:52:43	204.131.123.136	Emotet	Active	AS14061 DIGITLOCEAN-ASN	US
2021-01-26 06:51:41	204.131.144.150	Emotet	Active	AS14061 DIGITLOCEAN-ASN	US
2021-01-26 06:40:08	162.243.125.212	Emotet	Active	AS14061 DIGITLOCEAN-ASN	US
2021-01-26 06:39:44	40.105.131.87	Emotet	Active	AS16276 OVH	FR
2021-01-26 06:39:38	167.88.88.89	Emotet	Active	AS62187 CONTABO	DE
2021-01-26 06:39:35	85.234.143.94	Emotet	Active	AS29550 SIMPLYTRANSIT	GB
2021-01-26 06:38:04	91.76.28.129	Emotet	Active	AS16276 OVH	PL
2021-01-26 06:37:21	103.86.49.11	Emotet	Active	AS6865 BANGKOCENTERPRISE-TH Bangkok Enterprise Co., Ltd.	TH
2021-01-26 06:36:11	84.23.45.86	Emotet	Active	AS16276 OVH	FR
2021-01-26 06:30:58	88.148.263.191	Emotet	Active	AS8088 HKBN-AS-AP Hong Kong Broadband Network Ltd.	HK
2021-01-26 04:52:57	154.127.113.242	Emotet	Active	AS37058 BTOD	ZA
2021-01-26 12:02:33	195.243.194.77	Emotet	Active	AS13489 EPM Telecomunicaciones S.A. E.S.P.	CO
2021-01-26 11:26:47	76.133.4.236	Emotet	Active	AS3228 ALCOM	AX
2021-01-26 04:51:40	70.206.206.130	Emotet	Active	AS12302 PROxad	FR
2021-01-26 00:38:38	122.136.104.298	Emotet	Active	AS3462 Hinet Data Communication Business Group	TW
2021-01-24 03:27:13	123.176.76.234	Emotet	Active	AS7642 DHARAAGU-MIA-AP DEVIDE RAAJENSE GULSHN PLC	IN
2021-01-24 02:47:23	85.105.205.77	Emotet	Active	AS9323 TTNET	TR
2021-01-24 01:47:35	181.171.399.245	Emotet	Active	AS15328 Telefonos Argentina S.A.	AR
2021-01-23 20:57:33	10.61.114.36	Emotet	Active	AS33063 BNY-33063	US
2021-01-23 15:41:01	188.136.15.48	Emotet	Active	AS55000 NAWRAS-AS Sottolite of Onco	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

CREATORIdiFUTURO.it

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.