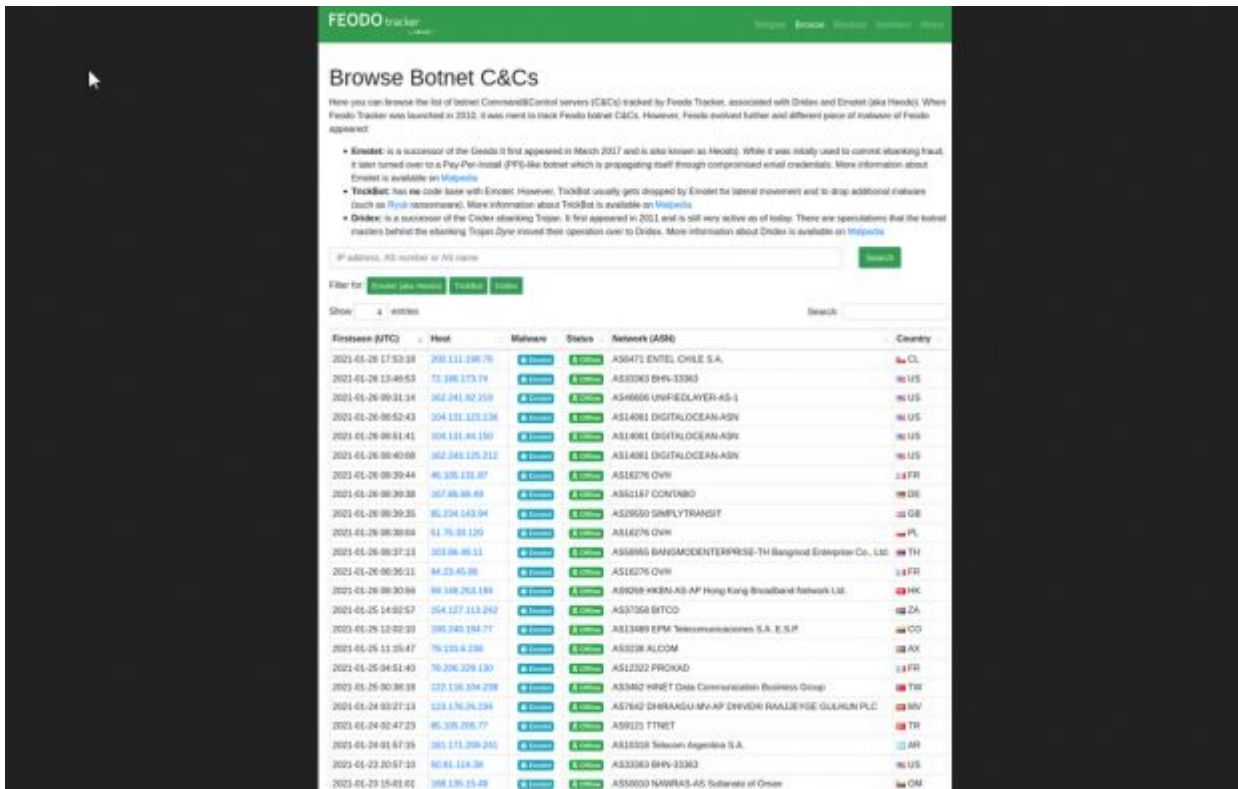


# Bye bye, Emotet



The screenshot shows the FEODO Tracker website, which is a platform for tracking botnet Command & Control (C&C) servers. The page title is "Browse Botnet C&Cs". Below the title, there is a brief description of the tracker and its purpose. A search bar is present, allowing users to filter by IP address, AS number, or AS name. The main content area displays a table of botnet C&Cs, with columns for Firstseen (UTC), Host, Malware, Status, Network (ASN), and Country. The table lists various botnet C&Cs, including those associated with Emotet, TrickBot, and others. The table is sorted by Firstseen (UTC) in descending order.

Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Country
2021-01-26 17:53:38	203.111.196.76	Emotet	Active	AS6471 ENTEL CHILE S.A.	CL
2021-01-26 13:49:53	72.188.173.74	Emotet	Active	AS3363 BNY-3363	US
2021-01-26 09:31:34	162.241.82.109	Emotet	Active	AS6666 UNF-ECLAYER-AS-1	US
2021-01-26 06:52:43	104.131.113.136	Emotet	Active	AS14061 DIGITLOCEAN-ASN	US
2021-01-26 06:51:41	104.131.113.150	Emotet	Active	AS14061 DIGITLOCEAN-ASN	US
2021-01-26 06:40:08	162.246.125.212	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	167.86.86.49	Emotet	Active	AS61167 CONTUNO	DE
2021-01-26 06:39:35	85.234.143.94	Emotet	Active	AS25500 SIMPLYTRANSIT	DE
2021-01-26 06:39:04	51.76.23.120	Emotet	Active	AS16276 OVH	PL
2021-01-26 06:37:11	163.86.46.51	Emotet	Active	AS58865 BANGKOCENTERPRISE-TH Bangkok Enterprise Co., Ltd.	TH
2021-01-26 06:36:11	84.23.45.88	Emotet	Active	AS16276 OVH	FR
2021-01-26 06:30:54	84.148.263.191	Emotet	Active	AS8268 HKBN-AS AP Hong Kong Broadband Network Ltd.	HK
2021-01-25 14:02:53	154.127.113.242	Emotet	Active	AS37058 BITOC	ZA
2021-01-25 12:02:33	185.243.194.71	Emotet	Active	AS13489 EPM Telecommunications S.A. E.S.P.	CO
2021-01-25 11:35:47	76.131.4.236	Emotet	Active	AS3238 ALCOM	AX
2021-01-25 04:51:43	70.206.328.130	Emotet	Active	AS12322 PROXAD	FR
2021-01-25 00:38:33	123.136.104.208	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 DHIRESH RAJAJEESE GULSHAN PLC	IN
2021-01-24 02:47:23	85.305.205.77	Emotet	Active	AS9323 TTNET	TR
2021-01-24 01:47:35	185.171.399.245	Emotet	Active	AS16328 Telecom Argentina S.A.	AR
2021-01-23 20:57:33	80.81.114.38	Emotet	Active	AS3363 BNY-3363	US
2021-01-23 15:01:01	188.136.15.49	Emotet	Active	AS55000 NAWELAS-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.

---

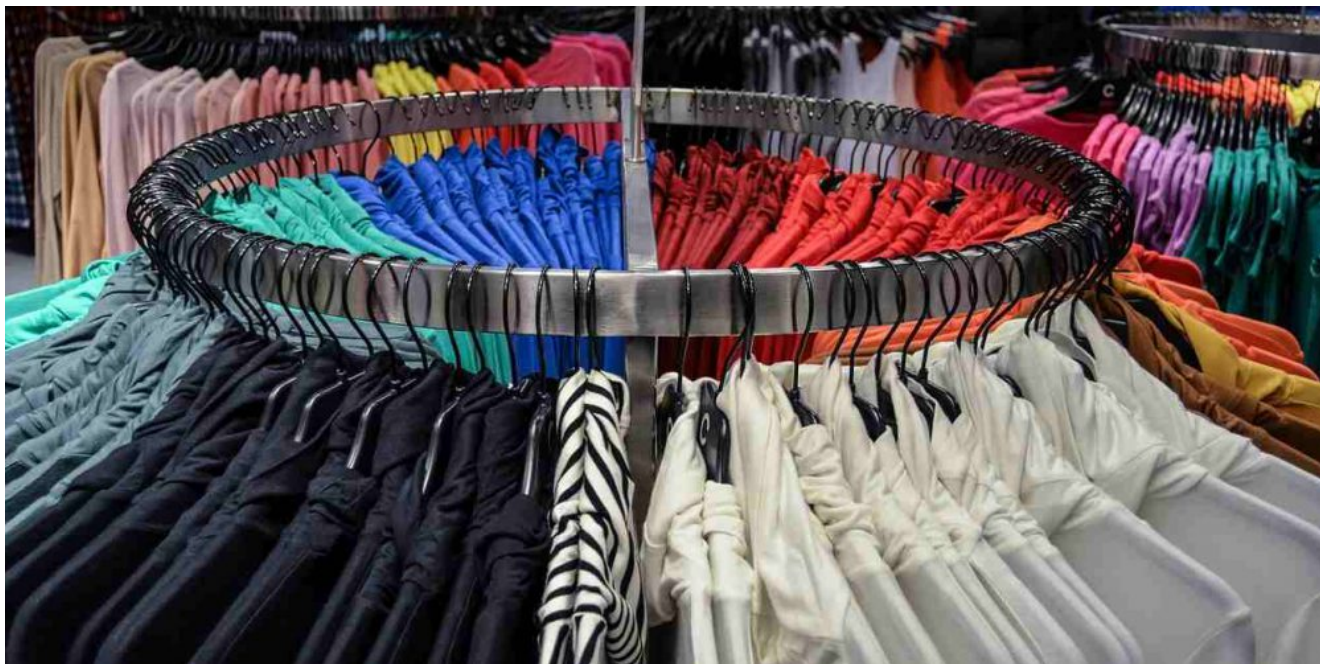
**Dalla CSR al CSV per  
perseguire un “successo  
sostenibile” e mitigare  
l'eco-ansia del consumatore**



Sostenibilità e transizione verso un'economia efficiente e circolare, adottando un approccio di condivisione del valore che permetta di superare le criticità, è cruciale per garantire la competitività a lungo termine

---

**“Le invio il mio avatar per le misure, va bene?” Dati e privacy in atelier**



Se noi avremo modo di trasferire al sistema di calcolo che guida l'avatar, sia nelle prime versioni puramente virtuali, che in quelle tridimensionali e materiali che Billy Berlusconi ci annuncia, i nostri dati psico-biologici, per rendere appunto il gemello in tutto corrispondente a noi via via che invecchiamo, a sua volta l'avatar a chi invierà questi dati preziosissimi per profilare intimamente l'umanità?

---

**Il Consiglio di sorveglianza di Facebook ha confermato il ban di Trump**





In una decisione rinviata da settimane e largamente attesa, l'Oversight Board ha escluso a tempo indeterminato l'ex presidente dai social network di Manlo Park. Con implicazioni importanti per le regole applicate ai politici sulla piattaforma

---

## Fenomeno Twitch



Piattaforma livestreaming generalista nata nel 2007 come Justin.tv, rinasce con uno sviluppo verticale focalizzato sui videogiochi nel 2014 come Twitch, quando Amazon l'acquista per 900 milioni di dollari. L'analisi del fenomeno di Sara Bassi per la rubrica #Ferpi2Be.