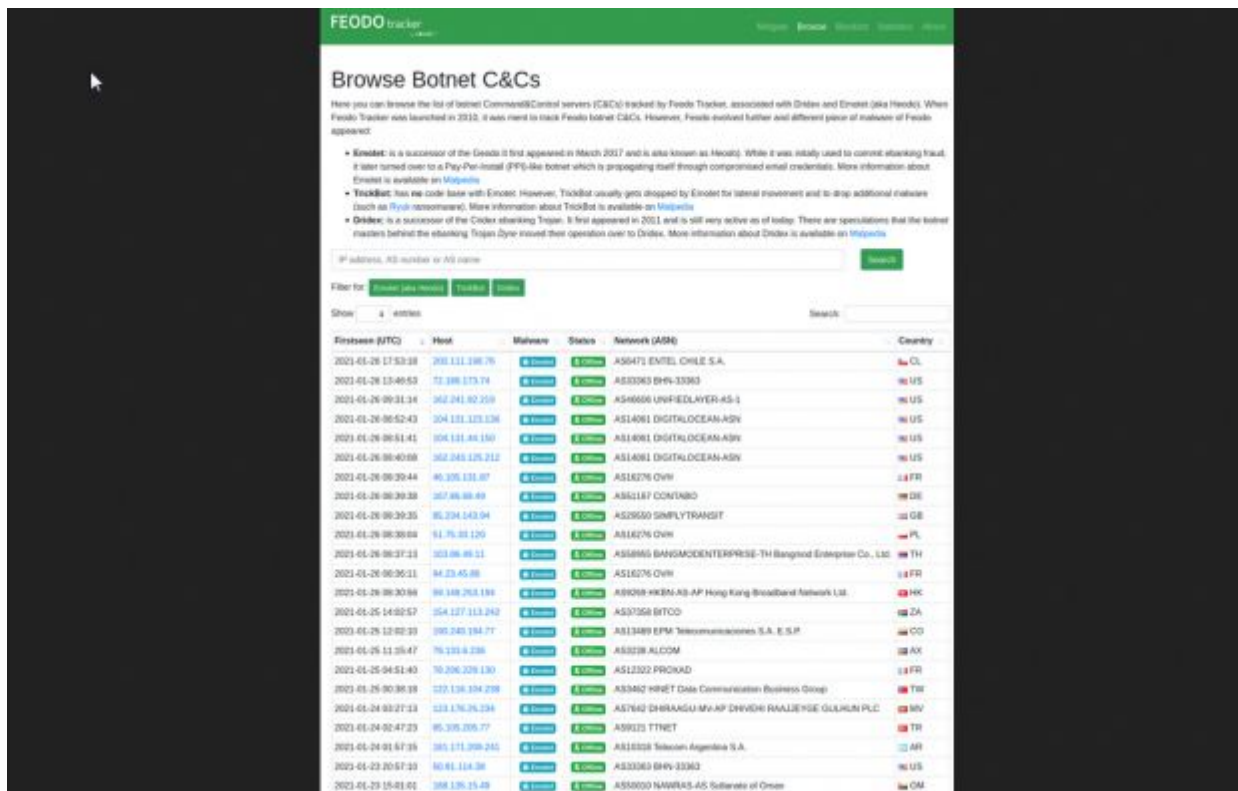


# Bye bye, Emotet



FEODO tracker

## Browse Botnet C&Cs

Here you can browse the list of botnet Command&Control servers (C&Cs) tracked by Feodo Tracker, associated with Dridex and Emotet (aka Hecot). When Feodo Tracker was launched in 2012, it was meant to track Feodo botnet C&C. However, Feodo evolved further and different pairs of malware of Feodo appeared:

- **Emotet**: is a successor of the Feodo II first appeared in March 2017 and is also known as Hecot. While it was initially used to control banking fraud, it later turned over to a Pay-Per-Install (PPI)-like botnet which is propagating itself through compromised email credentials. More information about Emotet is available on [Malpedia](#)
- **TrickBot**: has no code base with Emotet. However, TrickBot usually gets dropped by Emotet for lateral movement and to drop additional malware (such as [Ryuk ransomware](#)). More information about TrickBot is available on [Malpedia](#)
- **Dridex**: is a successor of the Cobas banking Trojan. It first appeared in 2011 and is still very active as of today. There are specializations that the botnet operators behind the banking Trojan Zyre moved their operation over to Dridex. More information about Dridex is available on [Malpedia](#)

IP address, AS number or AS name

Filter for: [Emotet \(aka Hecot\)](#) [TrickBot](#) [Dridex](#)

Show: 4 entries

Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Country
2021-01-26 17:53:28	203.121.236.76	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS6473 ENTEL CHILE S.A.	CL
2021-01-26 12:46:52	72.188.273.74	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS3263 BNY-3263	US
2021-01-26 09:31:34	362.241.92.259	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS4666 UNF-EDLAYER-AS-1	US
2021-01-26 06:52:43	204.121.123.126	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS14061 DIGITLOCEAN-ASN	US
2021-01-26 06:51:41	104.121.48.150	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS14061 DIGITLOCEAN-ASN	US
2021-01-26 06:40:68	362.240.126.212	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS14061 DIGITLOCEAN-ASN	US
2021-01-26 06:39:44	46.205.121.87	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS16276 OVH	FR
2021-01-26 06:39:38	257.86.88.49	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS61167 CONFIABO	DE
2021-01-26 06:39:35	85.234.143.94	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS2650 SIMPLYTRANSIT	DE
2021-01-26 06:39:04	51.76.83.120	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS16276 OVH	PL
2021-01-26 06:37:23	203.96.86.51	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS5865 BANGMAIDENTERPRISE-TH Bangkok Enterprise Co., Ltd	TH
2021-01-26 06:36:21	84.23.45.88	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS16276 OVH	FR
2021-01-26 06:30:59	99.148.253.191	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS8028 HKBN-AS-AP Hong Kong Broadband Network Ltd.	HK
2021-01-25 14:02:57	154.127.113.242	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS37058 BITOD	ZA
2021-01-25 12:02:33	185.240.194.77	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS13489 EPM Telefonoscomunicaciones S.A. E.S.P.	CO
2021-01-25 11:26:47	76.123.4.236	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS3228 ALICOM	AX
2021-01-25 04:51:43	70.204.226.130	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS12202 PROXAD	FR
2021-01-25 00:38:39	123.136.324.228	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS3462 HNET Data Communication Business Group	TR
2021-01-24 03:27:13	123.176.26.134	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS7642 DHRAAGU JV-AP DIVYSHI RAALIESE GULSHU PLC	IN
2021-01-24 02:47:23	85.205.205.77	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS8923 TTNET	TR
2021-01-24 01:57:35	185.171.209.245	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS18228 Telecom Argentina S.A.	AR
2021-01-23 20:57:23	80.81.124.38	<a href="#">Emotet</a>	<a href="#">Emotet</a>	AS3263 BNY-3263	US
2021-01-23 15:01:02	188.126.15.49	<a href="#">Emotet</a>	<a href="#">Emotet</a>	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.