

Bye bye, Emotet

Timestamp (UTC)	Host	Malware	Status	Network (ASN)	Country
2021-01-26 17:53:18	203.131.138.76	Emotet	Online	AS6471 ENTEL CHILE S.A.	CL
2021-01-26 13:46:53	73.188.173.74	Emotet	Online	AS33363 BHV-33363	US
2021-01-26 09:31:38	362.241.82.259	Emotet	Online	AS65656 UNIFIEDLAYER-AS-1	US
2021-01-26 06:52:43	204.131.123.138	Emotet	Online	AS14081 DIGITALOCEAN-ASN	US
2021-01-26 08:11:41	108.131.48.150	Emotet	Online	AS14081 DIGITALOCEAN-ASN	US
2021-01-26 08:40:08	362.245.125.212	Emotet	Online	AS14081 DIGITALOCEAN-ASN	US
2021-01-26 08:39:44	46.205.131.87	Emotet	Online	AS18276 GWR	FR
2021-01-26 08:39:38	267.86.88.89	Emotet	Online	AS62187 CONFABIO	DE
2021-01-26 08:39:35	85.234.143.08	Emotet	Online	AS28550 SINPLYTRANSIT	GB
2021-01-26 08:39:08	81.76.88.129	Emotet	Online	AS16276 GWR	PL
2021-01-26 08:37:18	103.08.88.11	Emotet	Online	AS53895 BANGMIDENTERPRISE-TH Bangkok Enterprise Co., Ltd	TH
2021-01-26 08:35:11	84.23.45.08	Emotet	Online	AS16276 GWR	FR
2021-01-26 08:30:04	80.148.283.188	Emotet	Online	AS1028-HKBN-AS-AP Hong Kong Broadband Network Ltd	HK
2021-01-25 14:02:57	354.127.113.242	Emotet	Online	AS53758 BTICO	ZA
2021-01-25 12:02:37	105.243.184.77	Emotet	Online	AS13489 EPM Telecomunicaciones S.A. E.S.P	CO
2021-01-25 11:26:47	76.123.8.236	Emotet	Online	AS32028 ALCOM	AX
2021-01-25 04:51:40	70.206.229.130	Emotet	Online	AS12502 PRICKAD	FR
2021-01-25 00:38:38	223.158.104.238	Emotet	Online	AS3402 HINET Data Communication Business Group	TR
2021-01-24 00:21:13	223.176.26.234	Emotet	Online	AS7642 DHIRANGU-MV-AP DHIRANGU RAJAEHSE GULHIN PLC	MV
2021-01-24 00:47:37	95.35.205.77	Emotet	Online	AS9933 TTNET	TR
2021-01-24 01:47:35	165.171.209.245	Emotet	Online	AS16208 Telecom Argentina S.A.	AR
2021-01-23 20:57:19	50.81.114.38	Emotet	Online	AS33363 BHV-33363	US
2021-01-23 15:01:01	108.139.135.48	Emotet	Online	AS58000 NAVARAS-US-Sellentele de Omnis	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 importante 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.