SPAMHAUS

Atualização sobre ameaças de botnet da Spamhaus

T1 2021

Após o encerramento (relativamente) mais tranquilo de 2020 para o mundo de botnet da Spamhaus, o primeiro trimestre começou em grande estilo. As principais notícias giraram em torno da eliminação da botnet Emotet em janeiro. Entretanto, quando um malware é derrubado, outro entra em cena, como prova o aumento de 24% no número total de botnet CCs que os pesquisadores da Spamhaus observaram.

Sejam bem-vindos à atualização sobre ameaças de botnet da Spamhaus para o 1º trimestre de 2021.

O que são controladores de botnet?

"Servidor comando e controle de botnet", "controlador de botnet" ou "botnet C2" são maneiras comuns de nos referirmos ao "botnet CC". Os fraudadores usam essa rede para controlar computadores infectados por malware e extrair valiosos dados pessoais das vítimas infectadas pelo malware.

Os botnet CCs desempenham um papel vital nas operações realizadas por cibercriminosos que usam computadores infectados para enviar spam ou ransomware, lançar ataques DDoS, aplicar golpes relacionados a bancos eletrônicos ou click fraud, ou minerar criptomoedas como bitcoins.

Computadores de mesa e dispositivos móveis, como smartphones, não são os únicos equipamentos que podem ser infectados. O número de dispositivos conectados à internet aumenta a cada dia, por exemplo, os dispositivos de Internet das Coisas (IoT), como webcams, unidades de armazenamento de dados em rede (NAS) e muitos outros.
Eles também correm o risco de serem infectados.

Destaque

O Emotet se foi, mas outras ameaças estão chegando

Em janeiro de 2021, uma coalizão internacional incluindo autoridades de vários países se encarregou de agir em âmbito global contra a famigerada botnet Emotet. Órgãos da segurança pública desarticularam a infraestrutura operada pela gangue Emotet, mandando para o espaço todo o tráfego da botnet Emotet.

A operação parece ter sido um sucesso. Ninguém foi preso em conexão com a operação, mas a botnet continua inativa há mais de dois meses. Entretanto, os especialistas da Spamhaus Malware Lab acreditam ser altamente provável que o Emotet volte a circular.

Durante os últimos anos, o Emotet frutificou, atraindo para si a bravata de ser uma das ameaças online mais perigosas. Os meliantes faziam dela uma base de operações para se infiltrar nas redes corporativas, movendo-se no interior da rede das vítimas e, em muitos casos, usando um ransomware para criptografá-la.

É duro admitir, mas as botnets não dão descanso: assim que uma botnet é eliminada, outra entra em ação. Sem muita demora, outros operadores de botnets correram para preencher o vazio que o Emotet deixou.

Durante o trimestre, meliantes operando botnets como IcedID, Dridex, Quakbot e TrickBot enviaram grandes volumes de e-mails de spam contendo documentos maliciosos. Na maioria das ameaças, o *modus operandi* é similar ao do Emotet: uma base de operações que dá acesso às redes corporativas e as criptografa com um ransomware.

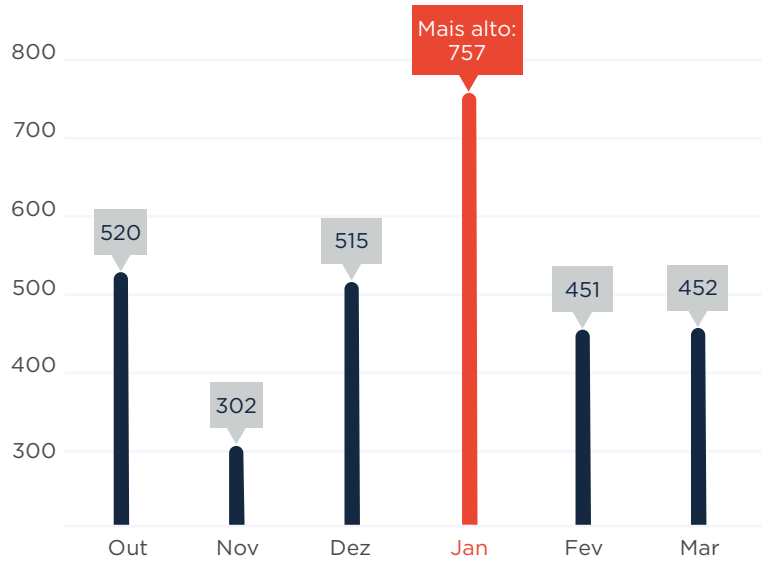
Emotet

O Emotet é um antigo cavalo de troia de banco eletrônico direcionado a clientes de e-banking no mundo todo. Em 2018, o Emotet encerrou suas atividades bancárias fraudulentas e começou a vender o acesso a computadores infectados.
A partir de 2019, o Emotet se transformou em uma das botnets mais perigosas.

Número de botnet CCs observados, T1 2021

Primeiro, vamos analisar o número de servidores de comando e controle (CCs) de botnet recém-observados no 1º trimestre de 2021. No total, a Spamhaus Malware Labs identificou 1.660 novos botnet CCs em comparação com 1.337 no 4º trimestre de 2020. Isso representa um aumento de 24%, com uma média de 553 botnet CCs por mês.

Número de novos botnet CCs detectados pela Spamhaus desde o final de 2020:



T4 Média mensal: 445

T1 Média mensal: 553

Geolocalização de botnet CCs, T1 2021

Em alguns países, temos visto um aumento nos novos casos de botnet CCs observados, enquanto outros países saíram da nossa lista dos Top 20.

Os Estados Unidos mantêm a 1ª posição

Apesar de uma pequena queda de 3% no número de botnets recém-observadas, os Estados Unidos continuam liderando o placar.

Aumentos na Europa

Os Países Baixos ultrapassaram a Rússia e agora ocupam a segunda posição, com um total de 207 botnets, um aumento de 27% em relação ao 4º trimestre de 2020.

Outros países europeus apresentaram um aumento em novas infraestruturas de botnet, incluindo a Alemanha (+77%), França (+82%), Suíça (+23%) e Reino Unido (+9%).

Novas entradas

Moldávia (nº 11), Hong Kong (nº 15), Argentina (nº 18), Colômbia (nº 18).

Partidas

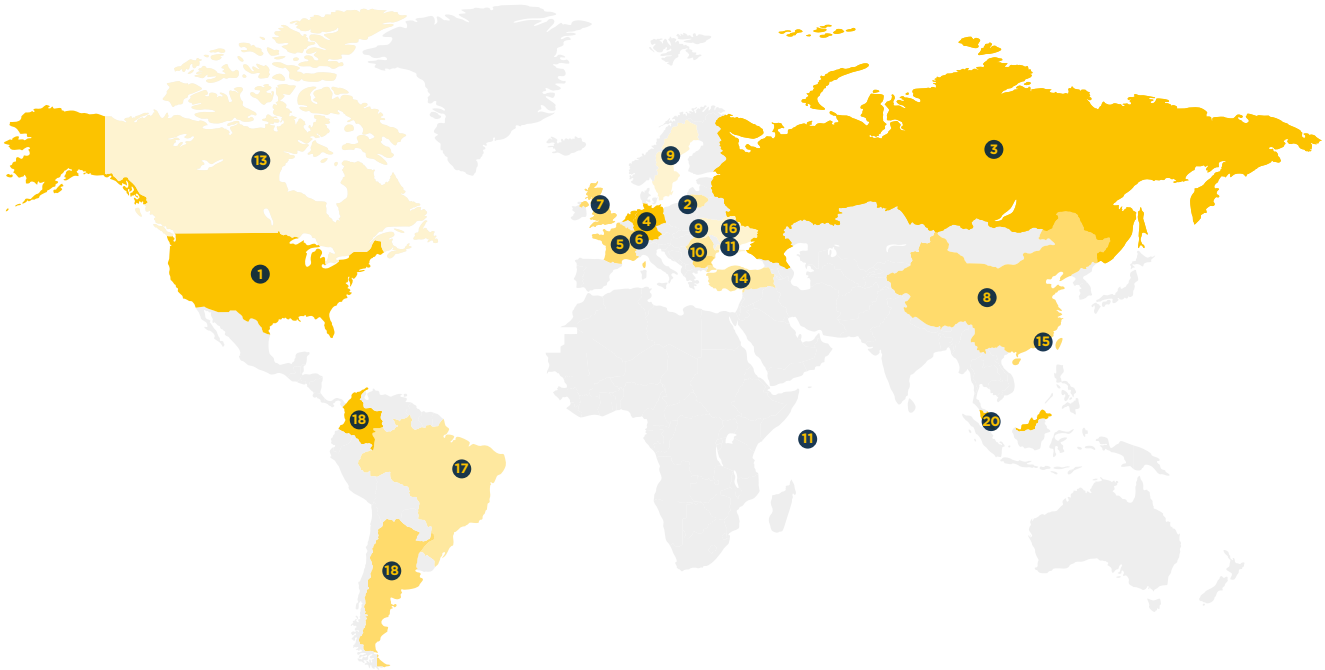
Bulgária, Hungria, Índia, Vietnã

Geolocalização de botnet CCs, T1 2021 (continuação)

Top 20 localizações de botnet CCs

Posição	País	T4 2020	T1 2021	Mudança % T a T
Nº 1	Estados Unidos	348	338	-3%
Nº 2	Países Baixos	163	207	27%
Nº 3	Rússia	247	195	-21%
Nº 4	Alemanha	56	99	77%
Nº 5	França	39	71	82%
Nº 6	Suíça	48	59	23%
Nº 7	Reino Unido	45	49	9%
Nº 8	China	32	42	31%
Nº 9	Suécia	34	39	15%
Nº 10	Letônia	24	31	29%

Posição	País	T4 2020	T1 2021	Mudança % T a T
Nº 11	Seychelles	10	29	190%
Nº 11	Moldávia	-	29	Nova entrada
Nº 13	Canadá	11	25	136%
Nº 14	Turquia	17	20	47%
Nº 15	Hong Kong	-	24	Nova entrada
Nº 16	Ucrânia	16	22	38%
Nº 17	Brasil	8	20	150%
Nº 18	Argentina	-	18	Nova entrada
Nº 18	Colômbia	-	18	Nova entrada
Nº 20	Singapura	31	16	-48%



Malware associado a botnet CCs, T1 2021

Emotet:

No 1º trimestre de 2021, o Emotet pulou para o topo da lista dos Top 20. Isso não foi surpresa, considerando nossos esforços em ajudar autoridades de segurança pública a desarticular a infraestrutura da botnet Emotet em janeiro de 2021.

Raccoon:

O Raccoon é um ladrão de credenciais novo na área. No 1º trimestre de 2021, identificamos 45 botnet CCs associados a esse novo malware.

FickerStealer:

Outro ladrão de credenciais observado pela primeira vez no 1º trimestre de 2021 foi o FickerStealer, com 25 novos botnet CCs associados.

QNodeService:

A primeira vez que vimos este malware foi em 2020. Contudo, parece que a atividade do QNodeService parou por completo no início do ano. Até o momento, não observamos nem um único CC associado a ele.

Novas entradas

Emotet (nº 1), Raccoon (nº 8), Gozi (nº 10), BitRat (nº 12), FickerStealer (nº 15), Vjw0rm (nº 17), TriumphLoader (nº 17), Hancitor (nº 20)

Partidas

Mirai, QNodeService, BazaLoader, ZLoader, CobaltStrike, Smoke Loader, Dridex, RevengeRAT

Malware associado a botnet CCs, T1 2021 (continuação)

Famílias de malware associadas a botnet CCs

Posição	T4 2020	T1 2021	Mudança %	Família de malware	Descrição
Nº 1	-	272	Nova entrada	Emotet	Instalador
Nº 2	53	124	134%	RemcosRAT	Ferramenta de acesso remoto (RAT)
Nº 3	164	83	-49%	Loki	Ladrão de credenciais
Nº 4	29	69	138%	AsyncRAT	Ferramenta de acesso remoto (RAT)
Nº 5	71	68	-4%	NanoCore	Ferramenta de acesso remoto (RAT)
Nº 6	66	55	-17%	RedLine	Ladrão de credenciais
Nº 6	93	55	-41%	AgentTesla	Ferramenta de acesso remoto (RAT)
Nº 8	-	45	Nova entrada	Raccoon	Ladrão de credenciais
Nº 9	17	39	129%	Arkei	Ladrão de credenciais
Nº 10	-	38	Nova entrada	Gozi	Cavalo de troia de banco eletrônico
Nº 11	30	36	20%	NjRAT	Ferramenta de acesso remoto (RAT)
Nº 12	21	33	57%	NetWire	Ferramenta de acesso remoto (RAT)
Nº 12	-	33	Nova entrada	BitRAT	Ferramenta de acesso remoto (RAT)
Nº 14	38	30	-21%	AveMaria	Ferramenta de acesso remoto (RAT)
Nº 15	-	25	Nova entrada	FickerStealer	Ladrão de credenciais
Nº 16	47	24	-49%	AZORult	Ladrão de credenciais
Nº 17	15	18	20%	QuasarRAT	Ferramenta de acesso remoto (RAT)
Nº 17	-	18	Nova entrada	Vjw0rm	Ladrão de credenciais
Nº 17	-	18	Nova entrada	TriumphLoader	Instalador
Nº 20	-	17	Nova entrada	Hancitor	Instalador

Domínios de nível superior (TLDs) mais explorados, T1 2021

Na classificação do T1 2021, o gTLD .com continua na liderança. A grande maioria dos domínios de botnet CC que a Spamhaus Malware Labs identificou estava hospedada nesse TLD. Contudo, vimos uma melhora na reputação de muitos outros TLDs listados — e eles caíram no placar.

.de:

Mais uma vez, o ccTLD da Alemanha entrou na lista dos Top 20, na 19ª posição. Isso não é bom! Será por causa de uma política antiexploração fraca na DENIC?

.top e .xyz:

Estes dois gTLDs têm uma longa história de uso indevido, e não surpreende que se mantenham entre os 5 principais — especialmente o .top, que teve 90% de aumento no número de botnet CCs hospedados no 1º trimestre de 2021.

Domínios de nível superior (TLDs) — uma breve apresentação

Existem vários domínios de nível superior (TLDs) diferentes, incluindo:

TLDs genéricos (gTLDs): podem ser usados por qualquer um

TLDs de código de país (ccTLDs): alguns têm uso restrito em um determinado país ou região, entretanto, outros são licenciados para uso geral, tendo a mesma funcionalidade dos gTLDs

TLDs descentralizados (dTLDs): domínios de nível superior (TLDs) independentes que não estão sob o controle da ICANN

Novas entradas

ru (nº 6), org (nº 10), biz (nº 12), us (nº 15), info (nº 18), co (nº 19), de (nº 19)

Partidas

casa, br, cyou, kr, ai, ac, gq

Domínios de nível superior (TLDs) mais explorados, T1 2021 (continuação)

Famílias de malware associadas a botnet CCs

Posição	T4 2020	T1 2021	Mudança %	TLD	Observação
Nº 1	2108	1549	-27%	com	gTLD
Nº 2	328	622	90%	top	gTLD
Nº 3	505	345	-32%	xyz	gTLD
Nº 4	141	124	-12%	tk	Originalmente ccTLD, agora efetivamente gTLD
Nº 5	185	121	-35%	ga	Originalmente ccTLD, agora efetivamente gTLD
Nº 6	-	114	Nova entrada	ru	ccTLD
Nº 7	100	108	8%	eu	ccTLD
Nº 8	133	106	-20%	ml	Originalmente ccTLD, agora efetivamente gTLD
Nº 9	95	87	-8%	me	gTLD
Nº 10	-	83	Nova entrada	org	gTLD
Nº 11	94	82	-13%	cf	Originalmente ccTLD, agora efetivamente gTLD
Nº 12	-	72	Nova entrada	biz	gTLD
Nº 12	81	72	-11%	net	gTLD
Nº 14	138	66	-52%	cc	gTLD
Nº 15	-	55	Nova entrada	us	ccTLD
Nº 16	77	51	-34%	su	ccTLD
Nº 17	74	47	-36%	la	ccTLD
Nº 18	-	46	Nova entrada	info	gTLD
Nº 19	-	36	Nova entrada	co	ccTLD
Nº 19	-	36	Nova entrada	de	ccTLD

Registradores de domínios mais explorados, T1 2021

Namecheap (de novo!)

Depois de anos na *pole position* dos Top 20, a Namecheap (EUA) continua sendo o registrador de domínios preferido entre os meliantes que registram domínios de botnet CCs.

Quando isso vai mudar? Não sabemos dizer. Mas dada a longa história de explorações da Namecheap, não parece que vai ser muito em breve, não!

Eranet International e RegRU

Com o aumento astronômico de 249%, a Eranet International (China) arrematou a 2º posição da NameSilo (Estados Unidos). Porém, a subida mais significativa no número de registros de domínio de botnet CC ficou com a RegRU (Rússia), com um aumento colossal de 341%.

Novas entradas

OnlineNIC (nº 13), name.com (nº 15), HiChina (nº 16), NameBright (nº 17)

Partidas

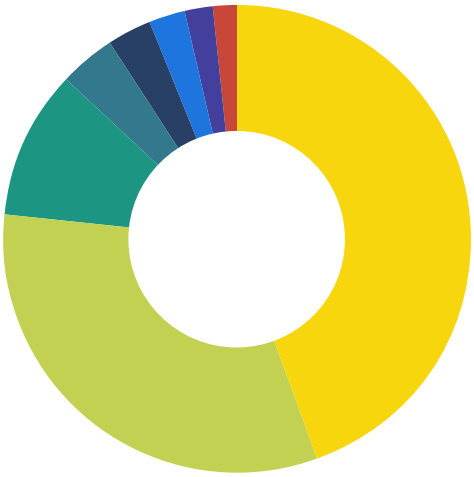
URL Solution, Hosting Concepts

Registradores de domínios mais explorados, T1 2021 (continuação)

Registradores de domínios mais explorados — número de domínios

Posição	T4 2020	T1 2021	Mudança %	Registrador	País
Nº 1	822	628	-24%	Namecheap	Estados Unidos
Nº 2	110	384	249%	Eranet International	China
Nº 3	444	259	-42%	NameSilo	Estados Unidos
Nº 4	54	238	341%	RegRU	Rússia
Nº 5	115	116	1%	55hl.com	China
Nº 6	101	85	-16%	Alibaba	China
Nº 7	343	72	-79%	PDR	Índia
Nº 8	367	59	-84%	Key Systems	Alemanha
Nº 9	111	56	-50%	WebNic.cc	Singapura
Nº 10	65	50	-23%	west263.com	China
Nº 11	25	44	76%	101Domain	Irlanda
Nº 12	48	42	-13%	Bizcn	China
Nº 13	-	38	Nova entrada	OnlineNIC	Estados Unidos
Nº 14	32	36	13%	OVH	França
Nº 15	-	35	Nova entrada	name.com	Estados Unidos
Nº 16	-	33	Nova entrada	HiChina	China
Nº 17	-	30	Nova entrada	NameBright	Estados Unidos
Nº 18	53	29	-45%	Tucows	Estados Unidos
Nº 19	46	28	-39%	1API	Alemanha
Nº 20	29	26	-10%	22net	China

LOCALIZAÇÃO DOS REGISTRADORES DE DOMÍNIOS MAIS EXPLORADOS



País	Botnets	%
Estados Unidos	1019	44,5%
China	736	32,2%
Rússia	238	10,4%
Alemanha	87	3,8%
Índia	72	3,1%
Singapura	56	2,4%
Irlanda	44	1,9%
França	36	1,6%

Redes que hospedam os mais novos botnet CCs recém-observados, T1 2021

Neste trimestre, vimos uma divisão entre leste e oeste, com uma redução no número de botnet CCs hospedados em provedores no leste, apenas para serem rapidamente substituídos pelos provedores de serviços de nuvem no oeste.

Provedores russos de VPS (servidor virtual privado)

Várias empresas, como a invs.ru e a selectel.ru, saíram da lista dos Top 20 este trimestre. Essa é uma excelente notícia, especialmente em relação à selectel.ru, que vem marcando presença na lista dos Top 20 há muito tempo.

Provedores de VPS na região oeste

Vários provedores localizados na região oeste entraram na lista dos Top 20 no T1 2021, incluindo google.com, choopa.com, hetzner.de e combahton.net.

A pior e a que apresentou os melhores resultados

A rede mais explorada é a privacyfirst.sh, um provedor de VPN que opera da Alemanha. Em contrapartida, a amazon.com reduziu o número de botnet CCs recém-observados na rede em 44% no decorrer do último trimestre. Um sinal bastante positivo!

Novas entradas

Google.com (nº 2), intersect.host (nº 6), choopa.com (nº 12) hetzner.de (nº 13), combahton.net (nº 13), linode.com (nº 16), ispserver.com (nº 17), colocrossing.com (nº 17), msk.host (nº 17)

Partidas

invs.ru, m247.ro, selectel.ru, namecheap.com, digitalocean.com, maxko.org, tencent.com, baxet.rubelcloud.net

[2]https://www.spamhaus.org/statistics/networks/

Redes que hospedam os mais novos botnet CCs recém-observados, T1 2021 (continuação)

Botnet CCs recém-observados por rede

Posição	T4 2020	T1 2021	Mudança %	Rede	País
Nº 1	106	131	24%	privacyfirst.sh	Alemanha
Nº 2	-	53	Nova entrada	google.com	Estados Unidos
Nº 3	33	51	55%	ovh.com	França
Nº 4	47	45	-4%	cloudflare.com	Estados Unidos
Nº 5	15	35	133%	pq.hosting	Moldávia
Nº 6	-	32	Nova entrada	intersect.host	Seychelles
Nº 7	55	31	-44%	amazon.com	Estados Unidos
Nº 8	45	28	-38%	endurance.com	Estados Unidos
Nº 9	26	26	0%	alibaba-inc.com	China
Nº 10	15	23	53%	itldc.com	Ucrânia
Nº 11	17	21	24%	serverion.com	Países Baixos
Nº 12	-	20	Nova entrada	choopa.com	Estados Unidos
Nº 13	-	19	Nova entrada	hetzner.de	Alemanha
Nº 13	-	19	Nova entrada	combahton.net	Alemanha
Nº 13	28	19	-32%	leaseweb.com	Países Baixos
Nº 16	-	18	Nova entrada	linode.com	Estados Unidos
Nº 17	-	17	Nova entrada	ispserver.com	Rússia
Nº 17	-	17	Nova entrada	colocrossing.com	Estados Unidos
Nº 17	25	17	-32%	dedipath.com	Estados Unidos
Nº 17	-	17	Nova entrada	msk.host	Rússia

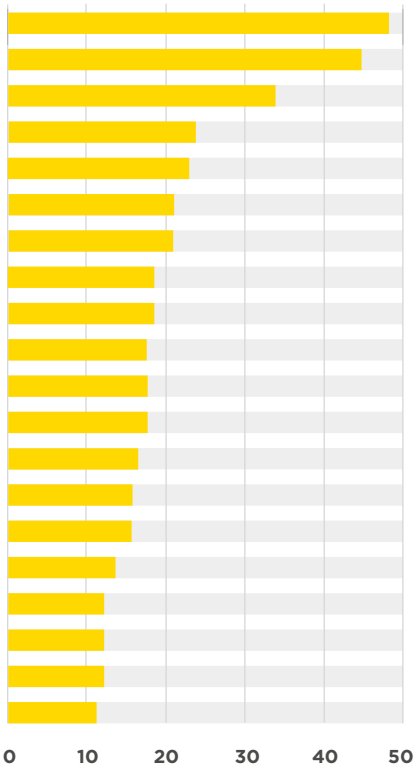
Redes que hospedam os botnet CCs mais ativos, T1 2021

Por último, mas não menos importante, vamos dar uma olhada nas redes que hospedaram de forma sistemática um grande número de botnet CCs ativos. Lamentavelmente, a Microsoft encabeça a lista das Top 20, com 48 botnet CCs ativos, seguida pela Google, com 43 botnet CCs ativos.

As redes que aparecem nessa lista demonstram ter uma higiene de rede insatisfatória e não agir quando recebem reclamações de uso indevido — a falta de mudança entre os últimos trimestres é um indicador. As botnets permanecem ativas por meses!

Número total de botnet CCs ativos por rede

Posição	T4 2020	T1 2021	Mudança %	Rede	País
Nº 1	48	48	0%	microsoft.com	Estados Unidos
Nº 2	43	43	0%	google.com	Estados Unidos
Nº 3	33	33	0%	ipjetable.net	Suíça
Nº 4	23	23	0%	ttnet.com.tr	Turquia
Nº 5	22	22	0%	charter.com	Estados Unidos
Nº 6	21	21	0%	inmotionhosting.com	Estados Unidos
Nº 6	21	21	0%	vietserver.vn	Vietnã
Nº 8	18	18	0%	claro.com.co	Colômbia
Nº 8	18	18	0%	cloudvider.net	Reino Unido
Nº 10	17	17	0%	ovpn.com	Suécia
Nº 10	17	17	0%	une.net.co	Colômbia
Nº 10	17	17	0%	datawire.ch	Suíça
Nº 13	16	16	0%	mail.ru	Rússia
Nº 14	14	14	0%	chinanet-js	China
Nº 14	14	14	0%	digitalocean.com	Estados Unidos
Nº 16	13	13	0%	mtnnigeria.net	Nigéria
Nº 17	12	12	0%	kornet.net	Coreia
Nº 17	12	12	0%	hostry.com	Chipre
Nº 19	12	11	-8%	eurobyte.ru	Rússia
Nº 19	11	11	0%	telstra.com	Austrália



Com os eventos relacionados ao Emotet no T1 2021, será interessante ver o que o próximo trimestre trará.

Até o trimestre que vem. Fiquem bem e protejam-se.