SPAMHAUS

Atualização sobre ameaças de botnet da Spamhaus

T2 2021

Neste trimestre, os pesquisadores da Spamhaus notaram uma redução de 12% em suas recentes observações de comando e controle (CC) de botnet, o que é uma boa notícia. Porém, a boa nova não vale para todos: mais de um provedor líder do setor está sofrendo com botnet CCs ativos em suas redes.

Sejam bem-vindos à atualização sobre ameaças de botnet da Spamhaus para o 2º 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

A história do Emotet continua

Sim, nós sabemos: mesmo tendo sido exterminado em janeiro, o Emotet continua em pauta. Isso porque a narrativa sobre o Emotet não acabou no momento de sua derrubada. Longe disso.

Como consequência da forma como o Emotet proliferou, através de *thread hijacking*, milhões de contas de e-mail foram comprometidas, ficando abertas para serem exploradas por outros malwares e ransomwares.

A Spamhaus passou o último trimestre trabalhando com o FBI para auxiliar nos esforços de remediação e alertas às pessoas afetadas. Temos aqui alguns números que dão uma ideia melhor do tamanho da operação:

- 1,3 milhão de e-mails comprometidos
- 22.000 domínios exclusivos
- 3.000 redes

Desde então, nossa equipe tem estado ocupada contatando as áreas exploradas, departamentos de confiança e segurança, e usuários finais, oferecendo-lhes dados para remediação e instruções sobre como proteger as contas comprometidas.

Temos o prazer de comunicar que mais de 60% das 1,3 milhão de contas estão, agora, em boas mãos. Isso mostra que todos temos um papel a cumprir como guardiões da internet.

O que é *thread hijacking*?

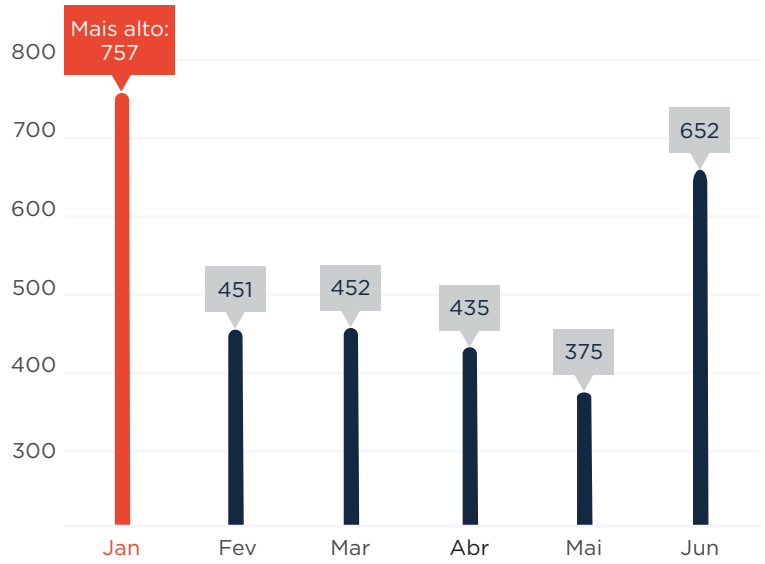
É quando os meliantes usam as conversas via e-mail (*threads*) existentes de suas vítimas para disseminar links ou anexos maliciosos para novas vítimas.

Um invasor pode ser extremamente convincente e enganar mais vítimas, fazendo com que cliquem em links nocivos ou baixem arquivos em resposta a uma sequência de e-mails existente.

Número de botnet CCs observados, T2 2021

Temos aqui uma visão geral do número de servidores de comando e controle (CCs) de botnet recém-observados no 2º trimestre de 2021. A Spamhaus Malware Labs identificou **1.462 botnet CCs** em comparação com 1.660 no 1º trimestre de 2021. Isso representa um **declínio** de **12%**. A média mensal de botnet CCs caiu de 553 no T1 para 487 no T2.

Número de novos botnet CCs detectados pela Spamhaus em 2021:



T1 Média mensal: 553

T2 Média mensal: 487

Geolocalização de botnet CCs, T2 2021

Vimos várias mudanças nas localizações geográficas que os cibercriminosos usaram para estabelecer novos servidores botnet CC, especialmente no fim da lista dos Top 20, onde houve uma enxurrada de novos participantes.

Queda na América Latina

Houve uma queda perceptível em países da América Latina que hospedam botnet CCs, com Argentina e Colômbia fora da lista dos Top 20 e o Brasil constatando uma queda de 40%. A única exceção foi o Panamá, que marca sua entrada na 13ª posição.

Aumento contínuo na Europa

Mais uma vez, constatamos um aumento no número de países europeus entrando na lista dos Top 20: República Tcheca, Polônia e Finlândia. Já Alemanha, França, Letônia e Reino Unido mostraram um aumento em botnet CCs.

Novas entradas

República Tcheca (nº 11), Panamá (nº 13), Malásia (nº 15), Polônia (nº 15), Finlândia (nº 17), Vietnã (nº 18).

Partidas

China, Suécia, Hong Kong, Argentina, Colômbia, Singapura.

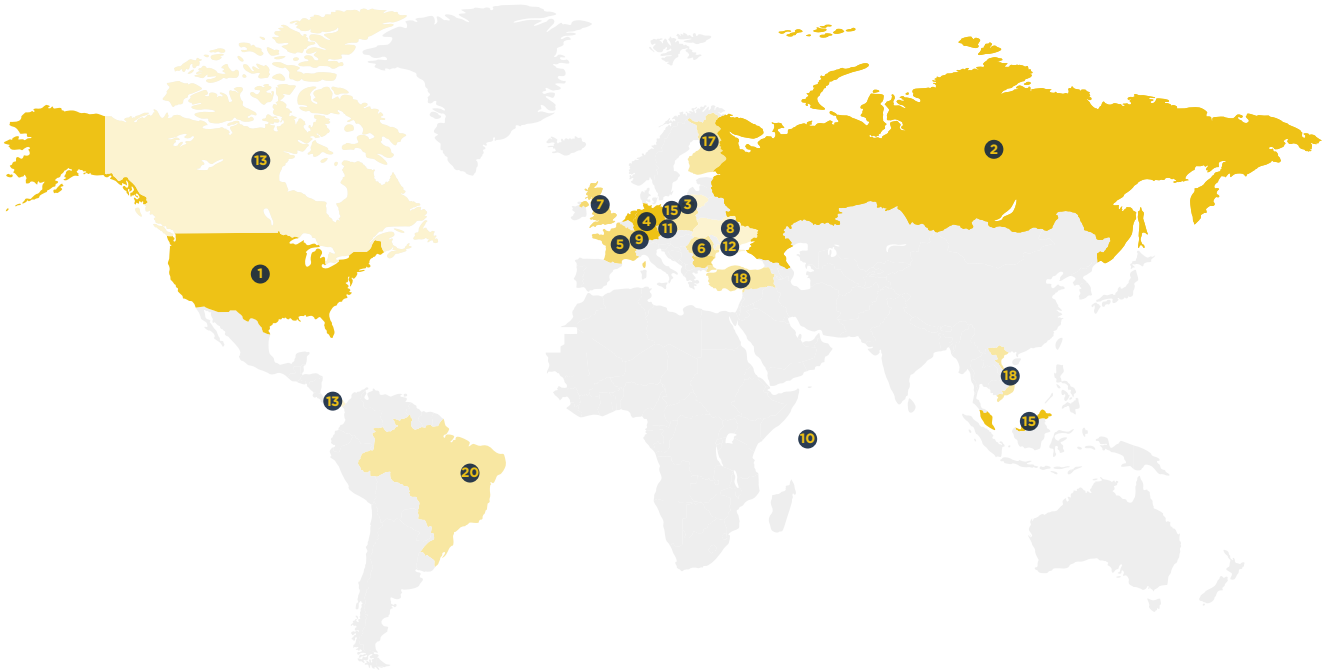
Geolocalização de botnet CCs, T2 2021 (continuação)

Top 20 localizações de botnet CCs

Posição	País	T1 2021	T2 2021	Mudança % T a T
Nº 1	Estados Unidos	338	281	-17%
Nº 2	Rússia	195	233	19%
Nº 3	Países Baixos	207	168	-19%
Nº 4	Alemanha	99	117	18%
Nº 5	França	71	92	30%
Nº 6	Letônia	31	84	171%
Nº 7	Reino Unido	49	57	16%
Nº 8	Ucrânia	22	44	100%
Nº 9	Suíça	59	41	-31%
Nº 10	Seychelles	29	38	31%

Nova entrada

Posição	País	T1 2021	T2 2021	Mudança % T a T
Nº 11	República Tcheca	-	31	Nova entrada
Nº 12	Moldávia	29	29	0%
Nº 13	Panamá	-	16	Nova entrada
Nº 13	Canadá	26	16	-38%
Nº 15	Malásia	-	15	Nova entrada
Nº 15	Polônia	-	15	Nova entrada
Nº 17	Finlândia	-	14	Nova entrada
Nº 18	Vietnã	-	13	Nova entrada
Nº 18	Turquia	25	13	-48%
Nº 20	Brasil	20	12	-40%



Malware associado a botnet CCs, T2 2021

Vamos começar com as boas novas. Após a derrota do tão falado botnet Emotet no 1º trimestre de 2021, temos o prazer de comunicar que não foi observada nenhuma atividade do Emotet.

Popularidade do instalador aumenta

No 2º trimestre, houve uma mudança de estratégia: de ladrões de credenciais e ferramentas de acesso remoto (RATs) para instaladores.

Raccoon chega rapidamente à primeira posição

O Raccoon só apareceu na lista dos Top 20 no último trimestre, na 8ª posição. No T2, ele subiu na classificação geral e assumiu a liderança.

Ladrões de credenciais à venda

O ladrão de credenciais Raccoon, mencionado acima, está à venda na dark web, assim como o RedLine e o Oski, que foram novas entradas em nossos gráficos do trimestre. Dada a facilidade de acesso, não surpreende ver a popularidade desse malware crescer.

O que é um instalador?

Os instaladores ocultam códigos para evitar que um malware seja detectado nas varreduras de vírus, ou seja, eles instalam o malware silenciosamente no sistema-alvo.

Novas entradas

Oski (nº 7), Tofsee (nº 11), STRRAT (nº 15), CryptBot (nº 16), CobaltStrike (nº 17), ServHelper (nº 18), IcedID (nº 18).

Partidas

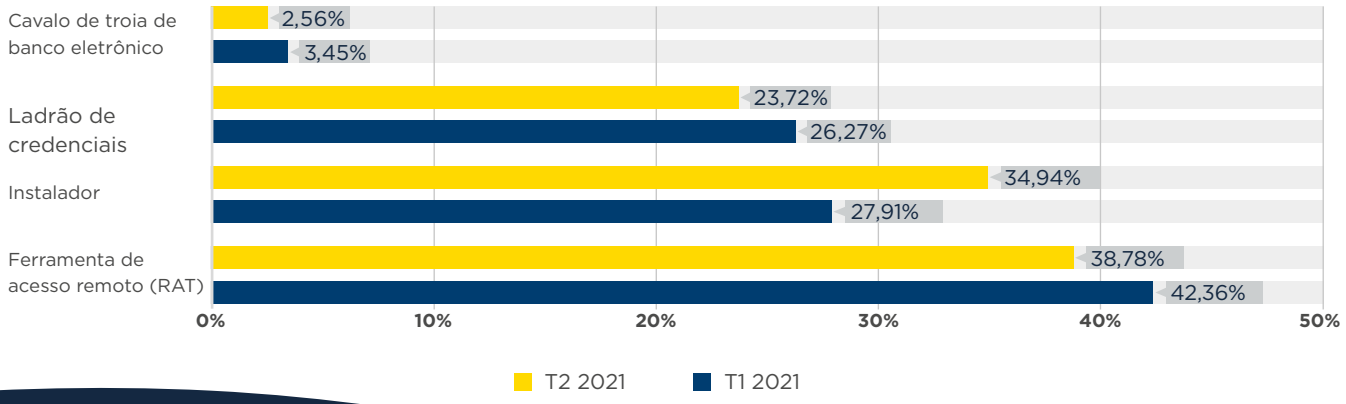
Emotet, NetWire, AveMaria, FickerStealer, AZORult, TriumpLoader, Hancitor

Malware associado a botnet CCs, T2 2021 (continuação)

Famílias de malware associadas a botnet CCs

Posição	T1 2021	T2 2021	Mudança %	Família de malware	Descrição
Nº 1	45	302	571%	Raccoon	Instalador
Nº 2	55	123	124%	RedLine	Ferramenta de acesso remoto (RAT)
Nº 3	69	83	20%	AsyncRAT	Ladrão de credenciais
Nº 4	83	66	-20%	Loki	Ferramenta de acesso remoto (RAT)
Nº 5	38	43	13%	Gozi	Ferramenta de acesso remoto (RAT)
Nº 6	33	42	27%	BitRAT	Ladrão de credenciais
Nº 7	-	28	Nova entrada	Oski	Ferramenta de acesso remoto (RAT)
Nº 8	18	26	44%	Vjw0rm	Ladrão de credenciais
Nº 9	36	24	-33%	NjRAT	Ladrão de credenciais
Nº 9	124	24	-81%	RemcosRAT	Cavalo de troia de banco eletrônico
Nº 11	68	23	-66%	NanoCore	Ferramenta de acesso remoto (RAT)
Nº 11	55	23	-58%	AgentTesla	Ferramenta de acesso remoto (RAT)
Nº 11	-	23	Nova entrada	Tofsee	Ferramenta de acesso remoto (RAT)
Nº 14	39	19	-51%	Arkei	Ferramenta de acesso remoto (RAT)
Nº 15	-	17	Nova entrada	STRRAT	Ladrão de credenciais
Nº 16	-	16	Nova entrada	CryptBot	Ladrão de credenciais
Nº 17	-	15	Nova entrada	CobaltStrike	Ferramenta de acesso remoto (RAT)
Nº 18	-	14	Nova entrada	ServHelper	Ladrão de credenciais
Nº 18	-	14	Nova entrada	IcedID	Instalador
Nº 20	18	11	-39%	QuasarRAT	Instalador

Comparações de tipos de malware entre T1 e T2 2021



Domínios de nível superior (TLDs) mais explorados, T2 2021

.com

Na classificação do T2 2021, o gTLD .com mais uma vez marcou presença no topo da lista. Além disso, o número de domínios de botnet CC recém-registrados que foi observado no .com aumentou em 166%, de 1.549 para 4.113!

.xyz

Com uma subida arrasadora de 114% no trimestre, não é de surpreender que o gTLD .xyz tenha tomado o lugar do gTLD .top e ocupe agora a 2ª posição.

TLDs de código de país

Apenas dois novos ccTLDs foram introduzidos na lista dos Top 20 desse trimestre: .br na 5ª posição e .cn na 12ª. Enquanto isso, três ccTLDs mostraram melhora na reputação e saíram da lista: .us, .de e .la.

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

buzz (nº 3), br (nº 5), VIP (nº 6), cloud (nº 10), cn (nº 12), online (nº 16), live (nº 17).

Partidas

me, biz, cc, us, la, co, de.

Domínios de nível superior (TLDs) mais explorados, T2 2021 (continuação)

TLDs mais explorados — número de domínios

Posição	T1 2021	T2 2021	Mudança %	TLD	Observação
Nº 1	1549	4113	166%	com	gTLD
Nº 2	345	739	114%	xyz	gTLD
Nº 3	-	662	Nova entrada	buzz	gTLD
Nº 4	622	607	-2%	top	gTLD
Nº 5	-	208	Nova entrada	br	ccTLD
Nº 6	-	175	Nova entrada	vip	gTLD
Nº 7	83	157	89%	org	gTLD
Nº 8	114	151	32%	ru	ccTLD
Nº 9	72	146	103%	net	gTLD
Nº 10	-	141	Nova entrada	cloud	gTLD
Nº 11	124	140	13%	tk	Originalmente ccTLD, agora efetivamente gTLD
Nº 12	-	139	Nova entrada	cn	ccTLD
Nº 12	108	116	7%	eu	ccTLD
Nº 14	121	106	-12%	ga	Originalmente ccTLD, agora efetivamente gTLD
Nº 15	106	104	-2%	ml	Originalmente ccTLD, agora efetivamente gTLD
Nº 16	-	86	Nova entrada	online	gTLD
Nº 17	-	81	Nova entrada	live	gTLD
Nº 18	51	80	57%	su	ccTLD
Nº 19	46	78	70%	info	gTLD
Nº 20	82	73	-11%	cf	ccTLD

Registradores de domínios mais explorados, T2 2021

Depois de muitos anos sem apresentar mudanças na classificação de reputação dos nossos registradores, finalmente estamos vendo um certo movimento!

NameSilo

Vimos o astronômico aumento de 594% no registro de novos domínios de botnet CC no registrador norte-americano de domínios NameSilo, tirando Namecheap da *pole position* no placar de classificação. Essa foi uma grande proeza, considerando-se que Namecheap teve um aumento de 52% nos domínios de botnet CC recém-registrados. Esses números são impressionantes!

Alemanha e China

Não foram apenas os registradores sediados nos EUA que viram aumentos significativos no T2. Os dois registradores de domínios sediados na Alemanha, Key Systems (56%) e 1API (254%), também sentiram o aumento no número de domínios de botnet registrados através de seus serviços, assim como quase todos os registradores chineses listados abaixo, incluindo a eName Technology, que entrou na nossa lista dos Top 20, ocupando a 3ª posição.

Novas entradas

eName Technology (nº 3), Arsys (nº 5), Xin Net (nº 10), CentralNic (nº 11), Network Solutions (nº 14).

Partidas

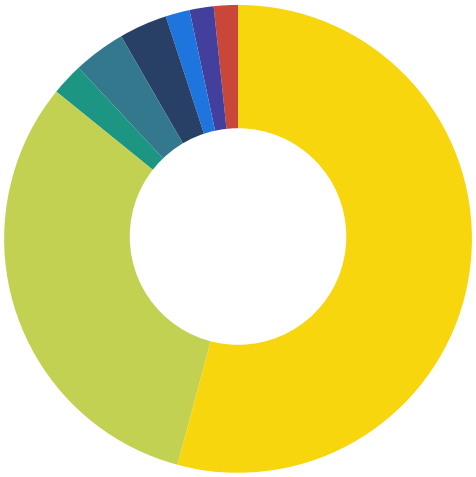
101 Domains, Bizcn, OnlineNIC, OVH, NameBright.

Registradores de domínios mais explorados, T2 2021 (continuação)

Registradores de domínios mais explorados — número de domínios

Posição	T1 2021	T2 2021	Mudança %	Registrador	País
Nº 1	259	1797	594%	NameSilo	Estados Unidos
Nº 2	628	955	52%	Namecheap	Estados Unidos
Nº 3	-	526	Nova entrada	eName Technology	China
Nº 4	85	504	493%	Alibaba	China
Nº 5	-	237	Nova entrada	Arsys	Espanha
Nº 6	384	215	-44%	Eranet International	China
Nº 7	72	188	161%	PDR	Índia
Nº 8	238	135	-43%	RegRU	Rússia
Nº 9	33	134	306%	HiChina	China
Nº 10	-	125	Nova entrada	Xin Net	China
Nº 11	-	112	Nova entrada	CentralNic	Reino Unido
Nº 12	26	110	323%	22net	China
Nº 12	29	110	279%	Tucows	Estados Unidos
Nº 14	-	101	Nova entrada	Network Solutions	Estados Unidos
Nº 15	28	99	254%	1API	Alemanha
Nº 16	59	92	56%	Key Systems	Alemanha
Nº 17	56	91	63%	WebNic.cc	Singapura
Nº 18	35	89	154%	Name.com	Estados Unidos
Nº 19	50	80	60%	west263.com	China
Nº 20	116	73	-37%	55hl.com	China

LOCALIZAÇÃO DOS REGISTRADORES DE DOMÍNIOS MAIS EXPLORADOS



País	Botnets	%
Estados Unidos	3052	52,9%
China	1767	30,6%
Espanha	237	2,3%
Alemanha	191	3,3%
Índia	188	3,3%
Rússia	135	1,6%
Reino Unido	112	1,6%
Singapura	91	1,6%
Total	5773	

Redes que hospedam os mais novos botnet CCs recém-observados, T2 2021

Há sempre muitas mudanças na hospedagem dos novos botnet CCs recém-observados, e esse trimestre não foi exceção.

Operação de hospedagem blindada

No T2, uma das maiores operações de hospedagem blindada mudou da Amazon para a DigitalOcean. O resultado foi uma rápida diminuição na quantidade de botnet CCs recém-observados na Amazon. Em contrapartida, houve um aumento repentino em novos botnet CCs hospedados na DigitalOcean.

Microsoft.com

Vimos a microsoft.com (EUA) entrar na lista dos Top 20. Observamos que ela hospeda uma quantidade significativa da infraestrutura dos botnet CCs Vjw0rm e BitRAT.

Novas entradas

nano.lv (nº 6), mgnhost.ru (nº 8), baxet.ru (nº 10), ipjetable.net (nº 11), digitalocean.com (nº 12), internet.it (nº 14), hostsailor.com (nº 16), microsoft.com (nº 17), m247.ro (nº 8), offshoreracks.com (nº 19), mivocloud.com (nº 19).

Partidas

intersec.host, amazon.com, endurance.com, choopa.com, combahton.net, leaseweb.com, linode.com, ispserver.com colocrossing.com, dedipath.com, msk.host.

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

Redes que hospedam os mais novos botnet CCs recém-observados, T2 2021 (continuação)

Botnet CCs recém-observados por rede

Posição	T1 2021	T2 2021	Mudança %	Rede	País
Nº 1	35	82	134%	pq.hosting	Rússia
Nº 2	53	74	40%	google.com	Estados Unidos
Nº 3	21	68	224%	serverion.com	Países Baixos
Nº 4	51	56	10%	ovh.com	França
Nº 5	23	53	130%	itldc.com	Ucrânia
Nº 6	-	49	Nova entrada	nano.lv	Letônia
Nº 7	131	48	-63%	privacyfirst.sh	Alemanha
Nº 8	-	47	Nova entrada	mgnhost.ru	Rússia
Nº 9	19	46	142%	hetzner.de	Alemanha
Nº 10	-	40	Nova entrada	baxet.ru	Rússia
Nº 11	-	35	Nova entrada	ipjetable.net	França
Nº 12	45	29	-36%	cloudflare.com	Estados Unidos
Nº 12	-	29	Nova entrada	digitalocean.com	Estados Unidos
Nº 14	-	28	Nova entrada	Internet.it	Rússia
Nº 15	26	26	0%	alibaba-inc.com	China
Nº 16	-	25	Nova entrada	hostsailor.com	Emirados Árabes
Nº 17	-	22	Nova entrada	microsoft.com	Estados Unidos
Nº 18	-	21	Nova entrada	m247.ro	Romênia
Nº 19	-	16	Nova entrada	offshoreracks.com	Panamá
Nº 19	-	16	Nova entrada	mivocloud.com	Moldávia

Redes que hospedam os botnet CCs mais ativos, T2 2021

Para finalizar, vamos dar uma olhada nas redes que hospedaram um grande número de botnet CCs ativos no 2º trimestre de 2021. Os provedores de hospedagem que aparecem nessa classificação têm um problema de exploração ou não tomam as medidas cabíveis quando recebem denúncias de uso indevido.

Eliteteam.to

Essa é uma empresa de hospedagem blindada que alega estar localizada em Seychelles. Na verdade, é mais que provável que operem da Rússia.

Microsoft.com e google.com

É evidente que a Microsoft está tendo dificuldades com a quantidade de situações de uso indevido geradas em sua plataforma em nuvem Azure. Da mesma forma, google.com é igualmente bombardeada por denúncias de uso indevido.

Parabéns aos que partiram!

Queremos cumprimentar a todos que saíram dessa lista — é bom ver o número de botnet CCs ativos diminuindo em suas redes. Bom trabalho!

Novas entradas

m247.ro (nº 12), eliteteam.to (nº 13), mgnhost.ru (nº 13), unusinc.com (nº 17).

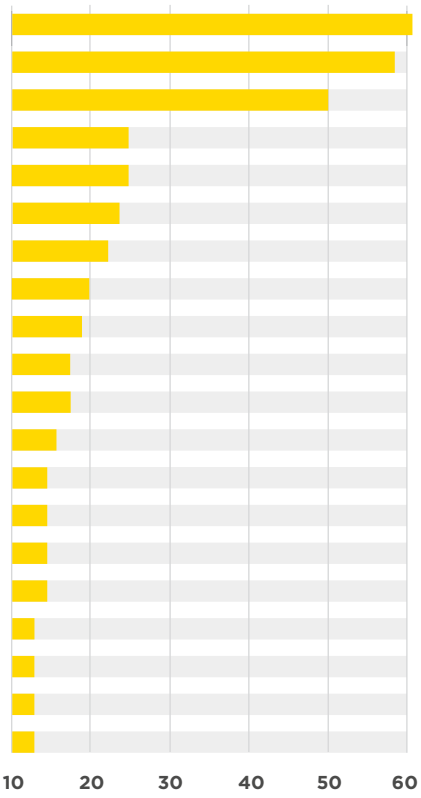
Partidas

mail.ru, digitalocean.com, eurobyte.ru, telstra.com.

Redes que hospedam os botnet CCs mais ativos, T2 2021 (continuação)

Número total de botnet CCs ativos por rede

Posição	T4 2020	T1 2021	Mudança %	Rede	País
Nº 1	33	61	85%	ipjetable.net	França
Nº 2	48	58	21%	microsoft.com	Estados Unidos
Nº 3	43	50	16%	google.com	Estados Unidos
Nº 4	23	23	0%	ttnet.com.tr	Turquia
Nº 4	21	23	10%	vietserver.vn	Vietnã
Nº 6	22	21	-5%	charter.com	Estados Unidos
Nº 6	21	21	0%	inmotionhosting.com	Estados Unidos
Nº 8	17	20	18%	ovpn.com	Suécia
Nº 9	18	18	0%	clouvider.net	Reino Unido
Nº 10	12	17	42%	hostry.com	Chipre
Nº 10	17	17	0%	une.net.co	Colômbia
Nº 12	-	15	Nova entrada	m247.ro	Romênia
Nº 13	17	13	-24%	datawire.ch	Suíça
Nº 13	-	13	Nova entrada	eliteteam.to	Seychelles
Nº 13	13	13	0%	mtnnigeria.net	Nigéria
Nº 13	-	13	Nova entrada	mgnhost.ru	Rússia
Nº 17	18	12	-33%	claro.com.co	Colômbia
Nº 17	12	12	0%	kornet.net	Coreia do Sul
Nº 17	14	12	-14%	chinanet-js	China
Nº 17	-	12	Nova entrada	unusinc.com	Estados Unidos



Por enquanto, é isso.

Protejam-se, e nos vemos em outubro!