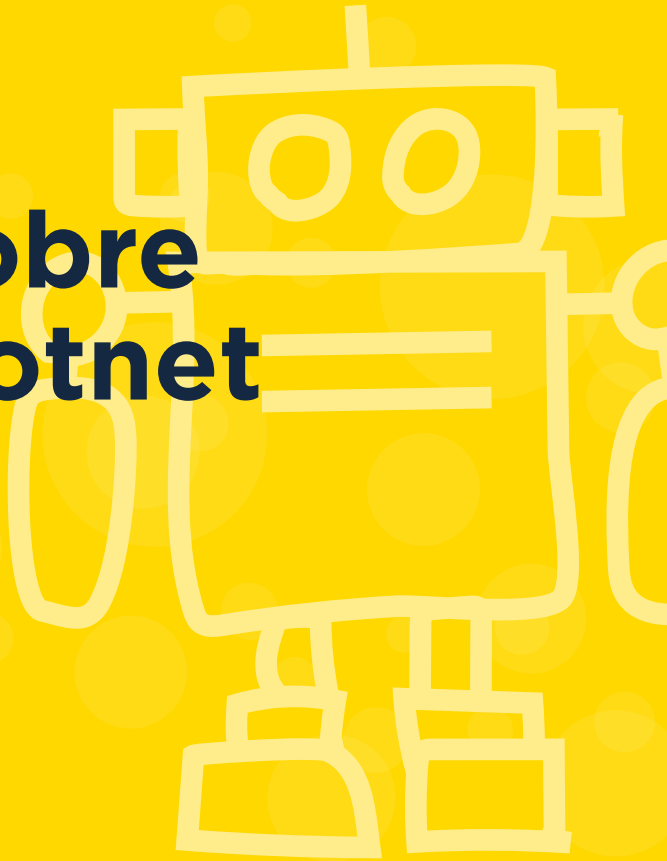
SPAMHAUS



Atualização sobre ameaças de botnet da Spamhaus

T4 2021

No 4º trimestre, registramos um aumento de 23% no número de novos comandos e controles (CCs) de botnet identificados por nossa equipe de pesquisadores. Apesar desse aumento, nossos pesquisadores estão cientes das atividades de botnet CC que eles não conseguem acompanhar devido ao modo de comunicação, que se dá via DNS por HTTPS (DoH). Isso é algo bastante preocupante, pois pende a balança a favor dos cibercriminosos.

Sejam bem-vindos à atualização sobre ameaças de botnet da Spamhaus para o 4º trimestre de 2021.

Sobre este relatório

A Spamhaus rastreia endereços de protocolo de internet (IP) e nomes de domínio usados por agentes de ameaças para hospedar servidores de comando e controle (CC) de botnet. Esses dados permitem que identifiquemos elementos associados, incluindo a geolocalização dos botnet CCs, o malware associado a eles, os domínios de nível superior (TLDs) usados ao registrar um domínio para um botnet CC, e os registradores que patrocinam e a rede que hospeda a infraestrutura do botnet CC.

Este relatório oferece uma visão geral sobre o número de botnet CCs associados a esses elementos, juntamente com uma comparação trimestral. Discutimos as tendências que observamos e destacamos provedores de serviços lutando para controlar o número de operadores de botnet que usam seus serviços indevidamente.

Destaque

Os problemas de DNS por HTTPS (DoH)

Vocês se lembram do FluBot e do TeamBot do 3º trimestre?

No último trimestre, registramos “um aumento repentino em malwares de backdoor” devido ao FluBot e ao TeamBot. No T4, com base na perspectiva da infraestrutura de botnet CC observada pela Spamhaus, essa família de malwares desapareceu completamente. Contudo, isso não significa que eles não estavam ativos. Muito pelo contrário — eles estavam!

Por que então eles não são detectados pela Spamhaus?

Esses malwares não aparecem em nossas listas porque os impostores responsáveis pelos ataques mudaram seus procedimentos operacionais. Em vez de estabelecer as comunicações de CC usando o protocolo HTTPS tradicional, eles usam DNS por HTTPS (DoH), utilizando indevidamente os grandes provedores de DoH, o que inclui Google e Alibaba.

Prevenir o uso abusivo da internet está mais difícil

Apesar de o DoH ter sido apresentado com toda a pompa e honra como o maior avanço em segurança da internet, alguns profissionais da área (incluindo a Spamhaus) demonstraram seu descontentamento ao se darem conta de que os bons perderiam ainda mais visibilidade sobre o que os maus estavam fazendo. E quando dizemos “ainda mais”, estamos nos referindo a outras questões, como a perda de visibilidade dos dados WHOIS.[1]

(1) www.spamhaus.org/news/article/775/how-has-gdpr-affected-spam

Por que o DoH é um problema?

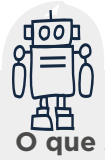
Com a criptografia do protocolo DoH, o tráfego DNS, que antes era público (não criptografado), passou a ser um recurso privado e protegido. Você pode achar que isso é algo bom, porém, como pode ver, nessas circunstâncias, os nossos pesquisadores não têm nenhuma visibilidade das solicitações de DNS do FluBot e do TeamBot. Consequentemente, não podemos listar os endereços IP, e assim os dados não podem ser usados para proteger os usuários. Ainda que o DoH tenha sido desenvolvido para proteger a comunidade da internet, ele também está dando corda para os cibercriminosos.
É uma faca de dois gumes.

O protocolo DoH não apenas torna a caça aos meliantes uma tarefa mais árdua, mas também faz com que a segurança dos produtos baseada no monitoramento e filtragem de DNS seja menos eficaz, o que está longe de ser benéfico. Os problemas de segurança são criados em sua maioria pelos provedores de DoH que não filtram as resoluções de DNS nocivas provenientes de domínios de botnet, phishing ou malware.

Número de botnet CCs observados, T4 2021

No 4º trimestre de 2021, a Spamhaus identificou 3.271 botnet CCs em comparação com 2.656 no 3º trimestre de 2021. Esse foi um aumento de 23% entre trimestres. A média mensal subiu de 885 no T3 para 1.090 botnet CCs por mês no T4.

Trimestre	Nº de botnets	Média trimestral	Mudança %
T1	1660	553	24%
T2	1462	487	-12%
T3	2656	885	82%
T4	3271	1090	23%



O que são controladores de botnet?

"Servidor de 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.

Geolocalização de botnet CCs, T4 2021

A Rússia continua com aumentos significativos

No trimestre passado, constatamos que o número de botnet CCs na Rússia aumentou drasticamente. Contudo, neste trimestre, vimos um aumento ainda maior:

- T1 para T2 – 19% de aumento
- T2 para T3 – 64% de aumento
- T3 para T4 – 124% de aumento

No 4º trimestre, quase 30% dos servidores de botnet CC estavam localizados na Rússia.

A América Latina continua presente

Vários países da América Latina (LatAm) entraram na lista no T3 e permaneceram entre os Top 20 no T4, incluindo México, República Dominicana, Brasil e Uruguai. O Uruguai apresentou o maior aumento percentual (181%) entre todas as localidades geográficas no 4º trimestre.

Altos e baixos na Europa

Após um aumento contínuo entre os vários países da Europa, temos o prazer de informar que vários deles apresentaram números reduzidos: os Países Baixos, a França, a Suécia e a Romênia. Já a Suíça saiu da lista dos Top 20 por completo. Contudo, a Alemanha ocupa agora a terceira posição, com um aumento de 35%, e a Grã-Bretanha apresentou um aumento de 56%.

Novas entradas

Ucrânia (nº 12), Bulgária (nº 15), Seychelles (nº 17), Hong Kong (nº 18).

Partidas

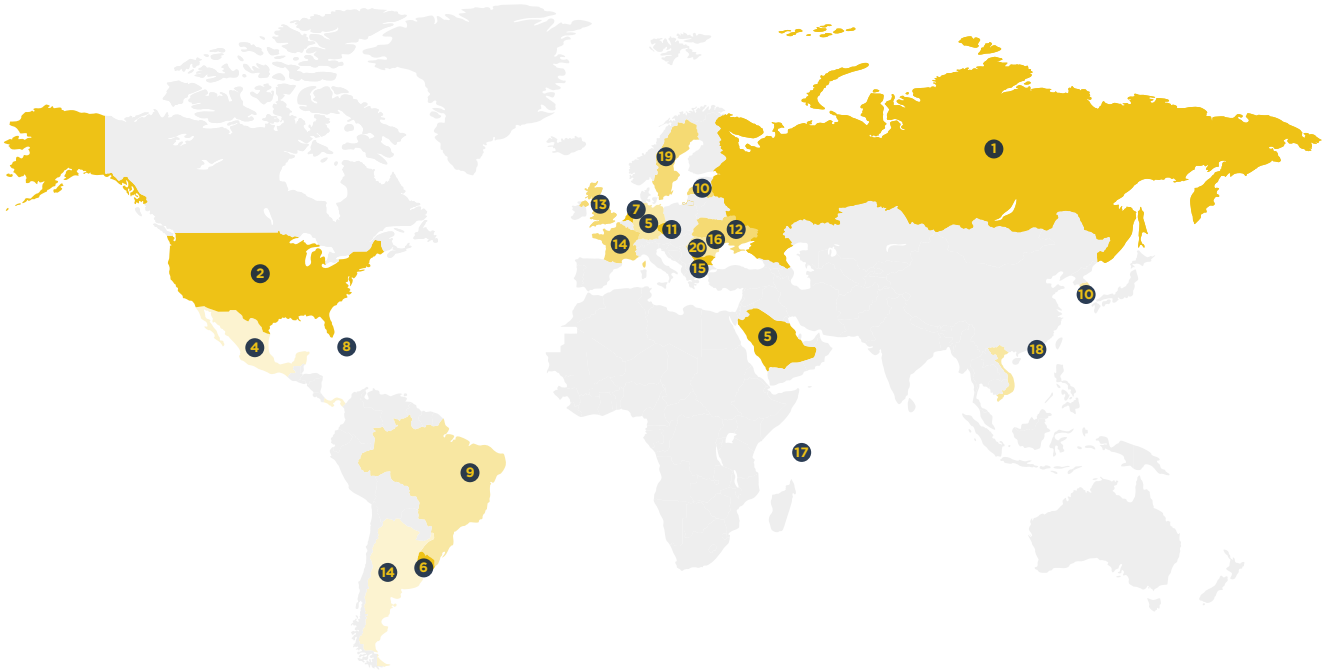
Coreia, Suíça, Argentina, Vietnã.

Geolocalização de botnet CCs, T4 2021 (continuação)

Top 20 localizações de botnet CCs

Posição	País	T3 2021	T4 2021	Mudança % T a T
Nº 1	Rússia	381	854	124%
Nº 2	Estados Unidos	301	384	28%
Nº 3	Alemanha	170	230	35%
Nº 4	México	182	186	2%
Nº 5	Arábia Saudita	117	180	54%
Nº 6	Uruguai	63	177	181%
Nº 7	Países Baixos	273	164	-40%
Nº 8	Rep. Dominicana	96	110	15%
Nº 9	Brasil	86	92	7%
Nº 10	Letônia	58	69	19%

Posição	País	T3 2021	T4 2021	Mudança % T a T
Nº 11	Rep. Tcheca	40	66	65%
Nº 12	Ucrânia	-	64	Nova entrada
Nº 13	Reino Unido	39	61	56%
Nº 14	França	123	60	-51%
Nº 15	Bulgária	-	56	Nova entrada
Nº 16	Moldávia	49	50	2%
Nº 17	Seychelles	-	34	Nova entrada
Nº 18	Hong Kong	-	28	Nova entrada
Nº 19	Suécia	38	26	-32%
Nº 20	Romênia	33	24	-27%



Malware associado a botnet CCs, T4 2021

Os ladrões de credenciais foram o tipo de malware mais predominante associado a botnet CCs no 4º trimestre. Isso não surpreende, visto que os dois principais malwares listados, RedLine e Loki, são ladrões de credenciais.

O surgimento do GCleaner

Vimos uma subida considerável nos índices de atividade do GCleaner, levando-o para a 4ª posição apesar de ser recém-chegado à lista dos Top 20. O GCleaner se assemelha ao Smoke Loader em seu *modus operandi*, sendo utilizado no modelo PPI (Pay-Per-Install), o que significa que ele instala outros malwares em hosts já infectados. Essa ameaça de malware já está na área há algum tempo, mas esta é a primeira vez que o GCleaner aparece na lista dos Top 20.

O desaparecimento do FluBot/TeamBot

Como tratado na seção "Destaque", esse malware que ocupava a 1ª colocação no trimestre passado desapareceu da nossa lista; porém, ele continua operacional e utiliza agora o protocolo DoH.

Novas entradas

GCleaner (nº 4), DCRat (nº 10), Arkei (nº 14), TrickBot (nº 15), Socelars (nº 16).

Partidas

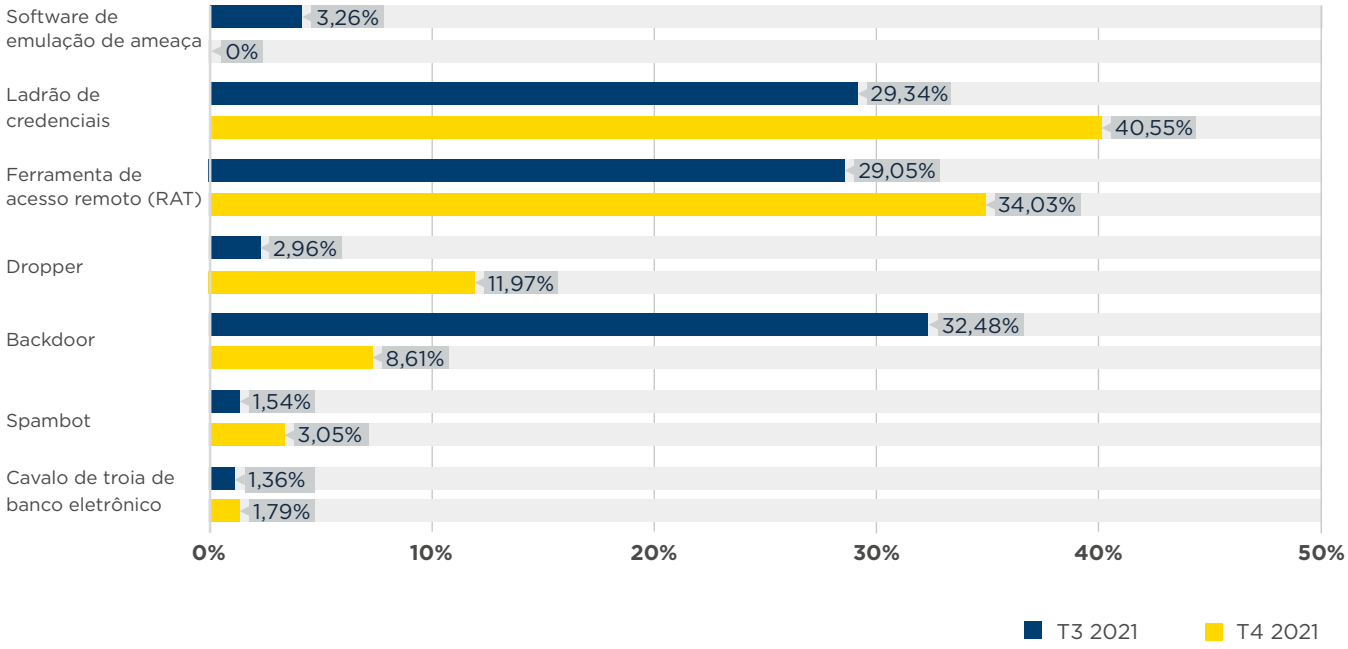
FluBot/TeamBot, AveMaria, ServHelper, QuasarRAT, AgentTesla.

Malware associado a botnet CCs, T4 2021 (continuação)

Famílias de malware associadas a botnet CCs

Posição	T3 2021	T4 2021	Mudança %	Família de malware	Descrição
Nº 1	210	164	-22%	RedLine	Ladrão de credenciais
Nº 2	108	102	-6%	Loki	Ladrão de credenciais
Nº 3	121	91	-25%	AsyncRAT	Ferramenta de acesso remoto (RAT)
Nº 4	-	86	Nova entrada	GCleaner	Dropper
Nº 5	93	75	-19%	Raccoon	Ladrão de credenciais
Nº 6	43	65	51%	Vjw0rm	Ferramenta de acesso remoto (RAT)
Nº 7	41	43	5%	CryptBot	Backdoor
Nº 8	136	37	-73%	BitRAT	Ferramenta de acesso remoto (RAT)
Nº 9	71	36	-49%	NjRAT	Ferramenta de acesso remoto (RAT)
Nº 10	-	32	Nova entrada	DCRat	Ferramenta de acesso remoto (RAT)
Nº 11	26	29	12%	Tofsee	Spambot
Nº 11	40	29	-28%	Remocs	Ferramenta de acesso remoto (RAT)
Nº 13	50	28	-44%	Smoke Loader	Dropper
Nº 14	-	27	Nova entrada	Arkei	Ladrão de credenciais
Nº 15	-	21	Nova entrada	TrickBot	Backdoor
Nº 16	-	18	Nova entrada	Socelars	Ladrão de credenciais
Nº 16	55	18	-67%	CobaltStrike	Backdoor
Nº 18	23	17	-26%	Gozi	Cavalo de troia de banco eletrônico
Nº 18	37	17	-54%	NanoCore	Ferramenta de acesso remoto (RAT)
Nº 18	30	17	-43%	STRRAT	Ferramenta de acesso remoto (RAT)

Comparações de tipos de malware entre T3 e T4 2021



Domínios de nível superior (TLDs) mais explorados, T4 2021

Uma nova entrada na 4ª posição

Em geral, não observamos novas entradas de TLD nas cinco principais posições do Top 20 desse botnet CC; contudo, o .xxx, um TLD direcionado a adultos, operado pelo ICM Registry, ocupa agora a 4ª posição. Com menos de 10.000 domínios ativos e um total de 223 domínios associados à atividade de botnet CC no 4º trimestre, só nos resta supor que temos um problema em mãos.

O .de reaparece

O ccTLD .de (Alemanha) reaparece em nossa classificação trimestral na 20ª posição desde seu desaparecimento do Top 20 no 2º trimestre.

Reduções e partidas

Gostaríamos de parabenizar todos os registradores que gerenciam os TLDs que abandonaram nossa lista e também aqueles que reduziram significativamente o número de botnet CCs associados que usam seus TLDs, incluindo .buzz e .net, os quais apresentaram uma redução de 80%.

Inexatidão de dados no T3

Queremos nos desculpar com a Verisign por um erro em nossas estatísticas do T3 2021 em relação ao .com. Informamos um número indevido de botnet CCs para o TLD, sendo que o valor correto foi de 3.730. Várias questões nos levaram a esse erro, mas confirmamos que já nos comunicamos com a Verisign para retificar a informação.

Interpretação dos dados

Registradores com um grande número de domínios ativos têm maior exposição ao uso abusivo. Por exemplo, no 4º trimestre de 2021, o .net teve mais de 13 milhões de zonas de domínio ativo, das quais 0,00103% foi associada a botnet CCs. Enquanto isso, o .xxx teve apenas um pouco mais de 9.000 domínios ativos, dos quais 2,4% foram associados a botnet CCs. Os dois se encontram entre os 10 primeiros colocados em nossa lista, ainda que um tenha tido um índice percentual muito mais elevado de domínios ativos associados a botnet CCs do que o outro.

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 ccTLDs 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.

Trabalhando juntos por uma internet mais segura

Obviamente, preferimos que os TLDs não tenham botnet CCs associados a eles, mas sabemos como é o mundo real e reconhecemos que teremos de conviver com os abusos.

O essencial é que tratemos os casos de uso abusivo com rapidez. Sempre que necessário, se os nomes de domínio forem registrados com o propósito único de distribuir malwares ou hospedar botnet CCs, gostaríamos que os registradores suspendessem esses nomes de domínio. Agradecemos os esforços dos muitos registradores que colaboram conosco para assegurar que essas ações sejam tomadas, incluindo .xyz e .top.

Novas entradas

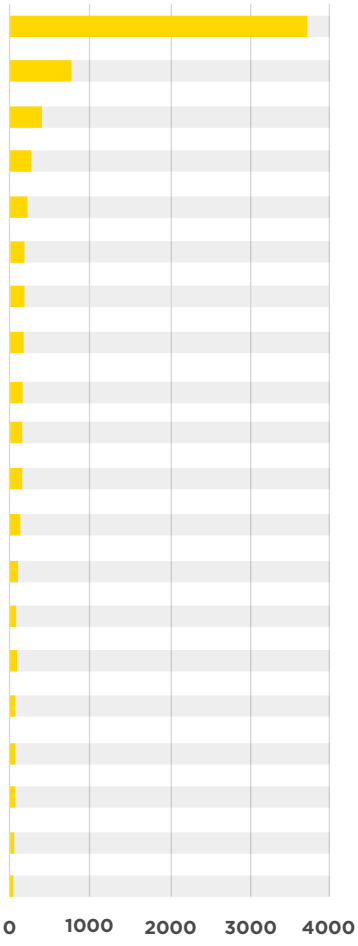
xxx (nº 4), site (nº 14), one (nº 15), gq (nº 16), sbs (nº 18), de (nº 20).

Partidas

cn, su, club, eu, co, monster.

TLDs mais explorados — número de domínios

Posição	T3 2021	T4 2021	Mudança %	TLD	Observação
Nº 1	3730	3719	-0,2%	com	gTLD
Nº 2	829	715	-14%	top	gTLD
Nº 3	833	396	-52%	xyz	gTLD
Nº 4	-	223	Nova entrada	xxx	gTLD
Nº 5	132	143	8%	ga	Originalmente ccTLD, agora efetivamente gTLD
Nº 6	665	136	-80%	net	gTLD
Nº 7	330	133	-60%	ru	ccTLD
Nº 8	183	122	-33%	tk	Originalmente ccTLD, agora efetivamente gTLD
Nº 9	265	116	-56%	org	gTLD
Nº 10	538	108	-80%	buzz	gTLD
Nº 11	178	103	-42%	info	gTLD
Nº 12	98	97	-1%	cf	Originalmente ccTLD, agora efetivamente gTLD
Nº 13	123	87	-29%	ml	Originalmente ccTLD, agora efetivamente gTLD
Nº 14	-	75	Nova entrada	site	gTLD
Nº 15	-	70	Nova entrada	one	gTLD
Nº 16	-	56	Nova entrada	gq	Originalmente ccTLD, agora efetivamente gTLD
Nº 17	82	52	-37%	cloud	gTLD
Nº 18	-	51	Nova entrada	sbs	gTLD
Nº 19	170	45	-74%	br	ccTLD
Nº 20	-	44	Nova entrada	de	ccTLD



Registradores de domínios mais explorados, T4 2021

No geral, vimos um decréscimo no registro de domínios fraudulentos no 4º trimestre de 2021, o que é uma boa notícia. Mas os registradores de alguns países continuam claramente enfrentando certas dificuldades.

Registradores baseados no Canadá

Os registradores no Canadá apresentaram os registros de botnet CC mais fraudulentos no T4, ultrapassando o índice apresentado pela China no T3.

Registradores baseados na Alemanha

Houve um aumento perceptível (136%) no número de botnet CCs associados a registradores que operam da Alemanha. Isso se deu devido à Key Systems, que enfrentou um aumento de 74%, e à 1API, que voltou a frequentar nossas listas na 12ª posição, depois de ter sido desbancada do Top 20 no T2.

Atak

Esse registrador de domínio surgiu pela primeira vez em nossas classificações. O Atak opera da Turquia e não respondeu a nenhuma de nossas denúncias de uso indevido até o momento. Assim, demos entrada em uma queixa na ICANN para a aplicação das medidas cabíveis contra o Atak. É imperativo que todos que formam a ecosfera da internet trabalhem juntos para proteger os usuários da internet.

Nicenic.net (China) e PDR (Índia)

Esses registradores apresentaram um aumento significativo no número de domínios de botnet CC registrados através deles no 4º trimestre. Contudo, ainda que os registros pelo PDR estejam aumentando, seu tempo de resposta em relação ao uso indevido é excelente.

Nossos agradecimentos a todos que saíram de nossas listas

No trimestre passado, destacamos que o CentralNic, West263 e Network Solutions tiveram problemas consideráveis com o aumento no número de domínios de botnet CC recém-registrados. No T4, todos os três registradores, juntamente com eName, Xin Net, 22net e OVH, saíram do Top 20 do trimestre, e queremos congratulá-los por seus esforços na prevenção de registros fraudulentos.

Registradores e operadores de botnet CC

Os cibercriminosos precisam encontrar um registrador patrocinador para registrar um nome de domínio para botnet CC. Não é fácil para os registradores detectarem todos os registros fraudulentos antes que esses domínios entrem em atividade. Entretanto, o "tempo de vida" de domínios criminosos em um registrador legítimo e bem-estruturado costuma ser relativamente curto.

Novas entradas

1API (nº 12), Beget (nº 14), Sav.com (nº 15), Hostinger (nº 16), Atak (nº 18), Naunet (nº 19), EuroDNS (nº 20), Mat Bao Corporation (nº 20).

Partidas

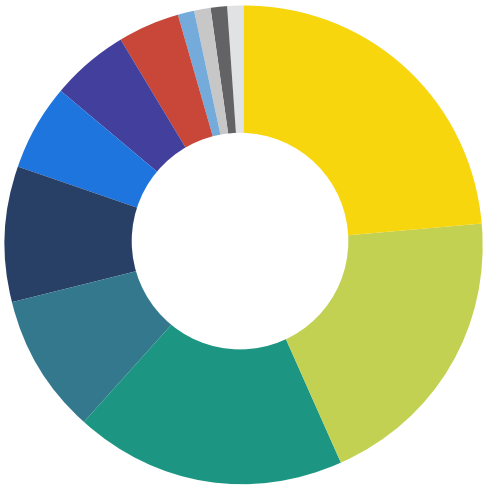
eName, CentralNic, Network Solutions, Xin Net, west263.com, 22net, OVH.

Registradores de domínios mais explorados, T4 2021 (continuação)

Registradores de domínios mais explorados — número de domínios

Posição	T3 2021	T4 2021	Mudança %	Registrador	País
Nº 1	1568	988	-37%	NameSilo	Canadá
Nº 2	1267	718	-43%	Namecheap	Estados Unidos
Nº 3	209	536	156%	nicenic.net	China
Nº 4	169	433	156%	PDR	Índia
Nº 5	188	328	74%	Key Systems	Alemanha
Nº 6	154	272	77%	WebNic.cc	Singapura
Nº 7	1217	201	-83%	Alibaba	China
Nº 8	165	197	19%	Openprovider	Países Baixos
Nº 9	189	135	-29%	Eranet International	China
Nº 10	403	127	-68%	Tucows	Canadá
Nº 11	475	124	-74%	RegRU	Rússia
Nº 12	-	115	Nova entrada	1API	Alemanha
Nº 13	403	80	-80%	Porkbun	Estados Unidos
Nº 14	-	68	Nova entrada	Beget LLC	Rússia
Nº 15	-	66	Nova entrada	Sav.com	Estados Unidos
Nº 16	-	57	Nova entrada	Hostinger	Lituânia
Nº 17	214	54	-75%	dnspod.cn	China
Nº 18	-	51	Nova entrada	Atak	Turquia
Nº 19	-	49	Nova entrada	NauNet	Rússia
Nº 20	-	48	Nova entrada	Mat Bao Corporation	Vietnã
Nº 20	-	48	Nova entrada	EuroDNS	Luxemburgo

LOCALIZAÇÃO DOS REGISTRADORES DE DOMÍNIOS MAIS EXPLORADOS



País	Botnets	%
Canadá	1115	23,75%
China	926	19,72%
Estados Unidos	864	18,40%
Alemanha	443	9,44%
Índia	433	9,22%
Singapura	272	5,79%
Rússia	241	5,13%
Países Baixos	197	4,20%
Lituânia	57	1,21%
Turquia	51	1,09%
Luxemburgo	48	1,02%
Vietnã	48	1,02%
Total	**4695**	

Redes que hospedam os mais novos botnet CCs recém-observados, T4 2021

Como de costume, ocorreram muitas mudanças nas redes que hospedam botnet CCs recém-observados.

Esta lista reflete a rapidez com que o problema de abuso é tratado nas redes?

Ainda que a lista das Top 20 ilustre que talvez haja um problema com o processo de averiguação dos clientes, ela não reflete a velocidade com que o pessoal de triagem lida com as denúncias recebidas de uso indevido.
Consulte "Redes que hospedam os botnet CCs mais ativos" para ver em quais redes os abusos não são tratados prontamente.

Um pouco de tudo

Uninet.net.mx (nº 1), serverion.com (nº 5) e cloudflare.com (nº 9) — todos os três aparecem entre os 10 primeiros em nossas listas, mas há grandes diferenças entre eles.

Uninet é um operador de telecomunicações e rede no México. Todos os botnet CCs recém-hospedados que identificamos em seu espaço de IP resultaram de equipamentos comprometidos de clientes.

Serverion é uma empresa de hospedagem sediada nos Países Baixos. Todos os botnet CCs que identificamos em sua rede no T4 resultaram de cadastros fraudulentos.

Por último, mas não menos importante, temos o Cloudflare, que não hospeda nenhum conteúdo, mas fornece um serviço de proxy reverso e proteção contra DDoS para botnet CCs, ocultando sua localização real.

Redes e operadores de botnet CC

As redes têm um controle razoável sobre os operadores que se cadastram fraudulentamente para receber um novo serviço.

Um processo de averiguação/avaliação criterioso deveria ocorrer antes de autorizar um serviço.

Quando as redes apresentam um grande número de entradas, isso ressalta um dos seguintes problemas:

1. As redes não estão seguindo as boas práticas no processo de averiguação do cliente.
2. As redes não estão assegurando que TODOS os seus revendedores sigam práticas sólidas de averiguação de clientes.

Em alguns dos piores cenários, funcionários ou proprietários de redes se beneficiam diretamente dos cadastros fraudulentos, ou seja, recebem dinheiro deliberadamente dos meliantes em troca da hospedagem de seus botnet CCs; felizmente, isso não acontece com muita frequência.

Novas entradas

selectel.ru (nº 10), timeweb.ru (nº 12), firstbyte.ru (nº 13), pinvds.com (nº 15), ihor-hosting.ru (nº 18), itldc.com (nº 19), m247.ro (nº 20).

Partidas

ipjetable.net, pq.hosting, ovh.com, mivocloud.com, telefonica.com.ar, uplus.co.kr, mgnhost.ru.

Redes que hospedam os mais novos botnet CCs recém-observados, T4 2021 (continuação)

Botnet CCs recém-observados por rede

Posição	T3 2021	T4 2021	Mudança %	Rede	País
Nº 1	177	187	6%	uninet.net.mx	México
Nº 2	33	182	452%	alibaba-inc.com	China
Nº 3	63	175	178%	antel.net.uy	Uruguai
Nº 4	105	168	60%	stc.com.sa	Arábia Saudita
Nº 5	115	116	1%	serverion.com	Países Baixos
Nº 6	95	110	16%	claro.com.do	Rep. Dominicana
Nº 7	58	85	47%	telefonica.com.br	Brasil
Nº 8	44	80	82%	baxet.ru	Rússia
Nº 9	68	72	6%	cloudflare.com	Estados Unidos
Nº 10	-	63	Nova entrada	selectel.ru	Rússia
Nº 11	44	51	16%	nano.lv	Letônia
Nº 12	-	49	Nova entrada	timeweb.ru	Rússia
Nº 13	-	48	Nova entrada	firstbyte.ru	Rússia
Nº 13	33	48	45%	hostwinds.com	Estados Unidos
Nº 15	-	47	Nova entrada	pinvds.com	Rússia
Nº 16	89	39	-56%	privacyfirst.sh	Alemanha
Nº 17	51	38	-25%	hetzner.de	Alemanha
Nº 18	-	36	Nova entrada	ihor-hosting.ru	Rússia
Nº 19	-	35	Nova entrada	itldc.com	Ucrânia
Nº 20	-	34	Nova entrada	m247.ro	Romênia

Redes que hospedam os botnet CCs mais ativos, T4 2021 (continuação)

Para finalizar, vamos rever as redes que hospedaram o maior número de botnet CCs ativos no fim de 2021. Os provedores de hospedagem que aparecem nessa classificação têm um problema de exploração, não tomam as medidas cabíveis quando recebem denúncias de uso indevido ou se omitem e não nos notificam quando solucionam um problema de uso indevido.

Novas entradas

al.bg (nº 8), mobily.com.sa (nº 12), ielo.net (nº 13), google.com (nº 16), combahton.net (nº 16).

Partidas

serverion.com, uplus.co.kr, hostry.com, skbroadband.com, claro.com.co.

Operadores de rede na região LatAm precisam abordar os problemas de uso abusivo rapidamente

Mais de 60% da lista de botnet CCs ativos ocorrem em redes localizadas na América Latina. Imploramos a esses operadores que respondam rapidamente às denúncias de uso indevido e colaborem com a Spamhaus para reduzir a exploração de botnet CC em suas redes.

Número total de botnet CCs ativos por rede (registrados até 31 de dezembro de 2021)

Posição	T3 2021	T4 2021	Mudança %	Rede	País
Nº 1	185	389	110%	uninet.net.mx	México
Nº 2	119	296	149%	stc.com.sa	Arábia Saudita
Nº 3	68	257	278%	antel.net.uy	Uruguai
Nº 4	97	204	110%	claro.com.do	Rep. Dominicana
Nº 5	63	146	132%	telefonica.com.br	Brasil
Nº 6	79	94	19%	microsoft.com	Estados Unidos
Nº 7	99	91	-8%	ipjetable.net	França
Nº 8	-	60	Nova entrada	a1.bg	Bulgária
Nº 9	41	41	0%	telefonica.com.ar	Argentina
Nº 10	29	29	0%	tie.cl	Chile
Nº 10	32	29	-9%	vietserver.vn	Vietnã
Nº 12	-	27	Nova entrada	mobily.com.sa	Arábia Saudita
Nº 13	-	25	Nova entrada	ielo.net	França
Nº 14	21	24	14%	clouvider.net	Reino Unido
Nº 15	24	22	-8%	ovpn.com	Suécia
Nº 16	22	21	-5%	charter.com	Estados Unidos
Nº 16	-	21	Nova entrada	google.com	Estados Unidos
Nº 16	21	21	0%	algartelecom.com.br	Brasil
Nº 16	21	21	0%	une.net.co	Colômbia
Nº 16	-	21	Nova entrada	combahton.net	Alemanha