SPAMHAUS

Atualização trimestral da reputação de domínio da Spamhaus

T2 2022

A Spamhaus, a líder independente em reputação de IPs e domínios, analisa a ecosfera de nomes de domínios. Do número de domínios recém-registrados até o uso abusivo de domínios que nossos pesquisadores estão observando, essa atualização destaca tendências, fornece insights sobre a baixa reputação dos domínios e defende os provedores quando são observadas melhorias.

Boas-vindas à Atualização trimestral da reputação de domínio da Spamhaus T2 2022.

Entrar

Conteúdo

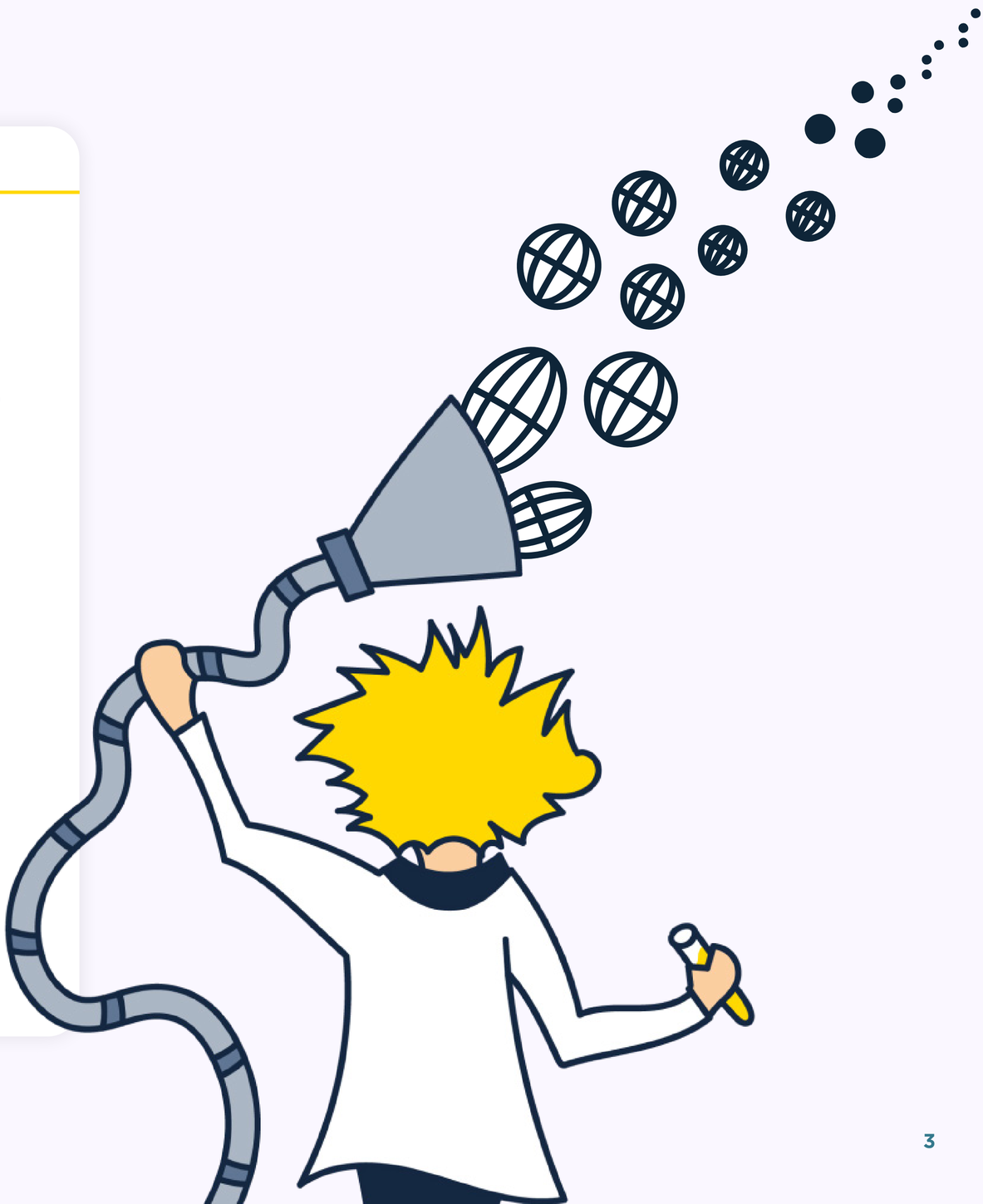
Apresentação geral

Por que examinamos os domínios e sua reputação associada? Por que faz sentido usar um nome de domínio como indicador de reputação ao filtrar decisões, quer essas decisões estejam relacionadas a e-mail, malware ou tráfego genérico da internet?

Os domínios têm um "formato" previsível, o que torna fácil extraí-los e agir de acordo com deles. Vários tipos de software de segurança são compatíveis com o uso de domínios (ou nomes de host) para destacar problemas e influenciar decisões. Isso não é uma grande surpresa, já que o Sistema de Nome de Domínio (DNS) é fundamental para quase tudo o que ocorre na internet e, em seu núcleo, "faz a associação entre várias informações atribuídas a nomes de domínios e cada entidade participante" (https://en.wikipedia.org/wiki/Domain_Name_System).

Não importa o que você está fazendo na internet, seja legítimo ou não, (quase sempre) é necessário usar um nome de domínio. Sem um nome de domínio, a maior parte da atividade maliciosa não começaria, muito menos teria sucesso.

Apresentação geral (continuação)



Apresentação geral (continuação)

Considere os seguintes cenários:

- Uma campanha de phishing por SMS usa um nome de domínio abreviado, comprado para esse objetivo (também conhecido como um registro malicioso), para direcionar os destinatários para um portal de pagamentos falso. Remova ou filtre o domínio, e a fraude não poderá ocorrer.
- Um malware tenta criar um canal de comando e controle usando um nome de domínio malicioso para contatar um servidor operado por um agente mal-intencionado. Retire o domínio, e não será possível estabelecer a comunicação.
- Um e-mail de spam forjado relacionado a drogas é enviado com todos os protocolos de autenticação corretamente configurados na mensagem (SPF, DKIM, DMARC). Mesmo que todos eles passem, saber que o domínio é malicioso criará um enorme sinal de alerta, e o e-mail será visto de forma diferente.

Agentes mal-intencionados experientes necessitam de nomes de domínio para cometer abusos: é simples assim. Alguns necessitam de centenas de domínios para evitar baixa reputação e listas de bloqueio; entretanto, alguns necessitam apenas de poucos provedores de serviços cuidadosamente selecionados, que não estão habituados a serem derrubados com rapidez.

Queremos chamar a atenção para esse tipo de atividade nefasta e dar destaque a provedores de serviços que vão muito além na tarefa de não oferecer um refúgio seguro para agentes mal-intencionados. Conforme publicarmos mais relatórios, esperamos continuar adicionando conteúdo para proporcionar contexto adicional e um maior insight para o mundo da reputação de domínio.

Novos domínios | Número de novos...

Novos domínios

Visão geral de novos domínios

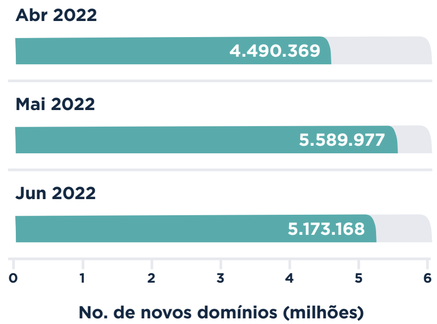
Um total de 15,3 milhões de novos domínios foram registrados no último trimestre, com uma média mensal de 5,1 milhões. Essa foi uma redução significativa de 43% em relação ao T1 deste ano, quando se observou 25,6 milhões de novos domínios.

Maio foi o mês mais agitado, com 5,6 milhões de domínios; entretanto, todos os três meses estiveram próximos à média mensal do trimestre, com variações mínimas.

É importante observar que um novo domínio não é um domínio suspeito *per se*. Entretanto, há uma quantidade considerável de uso abusivo associado a novos nomes de domínio. Um motivo é que se um agente mal-intencionado comprar um novo domínio e o usar imediatamente, haverá pouquíssima chance de que os sistemas e profissionais de segurança tenham conhecimento prévio da existência desse domínio. Infelizmente, sua existência só será descoberta após a campanha maliciosa ter começado. Além disso, ao usar novos domínios, os agentes mal-intencionados impedem que os registros e registradores realizem derrubadas preventivas.

Novos domínios | Número de novos...

Número de novos domínios por mês



Total do trimestre
15.253.514
▼-43%▼

Média mensal
5.084.505
▼-3.764.414▼

O que é um novo domínio?

A Spamhaus classifica um “novo domínio” como um domínio que foi recém-registrado ou recém-observado e que está listado pela Spamhaus para um período de 24 horas em seu dataset de Domínio de Reputação Zero (ZRD). Domínios recém-criados raramente são usados para finalidades legítimas dentro de 24 horas após seu registro; entretanto, os cibercriminosos registram e “queimam“ centenas de domínios diariamente. Quando esses novos domínios são vistos em ação, esse é um forte indicador de um possível comportamento malicioso.

A equipe de pesquisa compila essa lista a partir de várias fontes de dados, incluindo Passive DNS, dados de SMTP e arquivos de zonas compartilhados pelos registros. Portanto, os dados de novos domínios não são o número exato de novos domínios, mas o número de novos domínios dos quais a Spamhaus tem visibilidade.

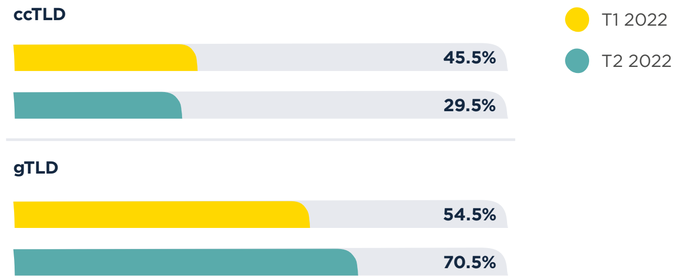
Novos domínios por domínio de nível superior (TLD)

Todos os TLDs que saíram do Top 20 no T2 eram ccTLDs. Com isso em mente, não será surpresa ver que os tipos de TLDs demonstram que os ccTLDs diminuíram em mais de 15% no T2.

Você observará que alguns gTLDs tiveram um enorme aumento no número de novos domínios em suas zonas em comparação com o trimestre anterior. Por exemplo, .xyz teve um gigantesco aumento de 4301%. Em alguns casos, é possível traçar o aumento de popularidade de alguns domínios gTLDs até promoções realizadas pelo TLD. Os registros podem realizar essas promoções com todos os seus registradores ou com apenas alguns selecionados.

Como a maioria dessas promoções reduz drasticamente o preço (uma redução de 90% não é incomum!), um registrante consegue comprar muito mais domínios pela mesma quantia. Isso é extremamente atraente, não apenas para os especuladores de nomes de domínios, mas também para os agentes mal-intencionados, que ”queimam” domínios como parte de seu “modelo de negócios”.

Comparação de tipos de TLDs de novos domínios, por trimestre



Domínios de nível superior (TLDs) — uma breve explicação

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

- **TLDs genéricos (gTLDs) —** estão sob jurisdição da ICANN. Alguns gTLDs são abertos, ou seja, podem ser usados por qualquer pessoa (por exemplo, .com), alguns têm políticas rigorosas que regulam quem pode usá-los e como (por exemplo, .bank) e alguns são fechados (por exemplo, .honda).
- **TLDs de código de país (ccTLDs) —** normalmente, estão relacionados a um país ou região. Os registros definem as políticas relacionadas a esses TLDs; alguns permitem que sejam feitos registros provenientes de qualquer lugar, alguns exigem presença local e alguns licenciam seu namespace indiscriminadamente para outros.

Top 20 TLDs... | Top 20 ccTLDs...

Top 20 TLDs usados em novos domínios

Posição	TLD de novo domínio	Tipo de TLD	T2 2022	Barra de dados do T2	T1 2022	Mudança %
1	.com	gTLD	5.750.666		6.049.245	▼ -5%
2	.xyz	gTLD	503.191		-	Nova entrada
3	.net	gTLD	291.331		148.871	▲ 96%
4	.cn	ccTLD	279.479		358.472	▼ -22%
5	.de	ccTLD	267.250		444.562	▼ -40%
6	.org	gTLD	263.430		141.957	▲ 86%
7	.online	gTLD	238.194		-	Nova entrada
8	.tk	ccTLD	228.359		660.463	▼ -65%
9	.top	gTLD	203.738		-	Nova entrada
10	.ga	ccTLD	183.826		312.729	▼ -41%
11	.ml	ccTLD	177.008		305.437	▼ -42%
12	.shop	gTLD	172.363		-	Nova entrada
13	.nl	ccTLD	150.862		199.900	▼ -25%
14	.site	gTLD	145.313		-	Nova entrada
15	.co.uk	ccTLD	130.201		228.559	▼ -43%
16	.info	gTLD	127.696		-	Nova entrada
17	.com.br	ccTLD	121.371		224.770	▼ -46%
18	.ru	ccTLD	107.452		208.810	▼ -49%
19	.store	gTLD	102.916		-	Nova entrada
20	.eu	ccTLD	102.454		125.592	▼ -18%

0 2 4 6

Top 20 TLDs... | Top 20 ccTLDs...

Top 20 ccTLDs usados em novos domínios

Posição	TLD de novo domínio	T2 2022	Barra de dados do T2	T1 2022	Mudança %
1	.cn	279.479		358.472	▼ -22%
2	.de	267.250		444.562	▼ -40%
3	.tk	228.359		660.463	▼ -65%
4	.ga	183.826		312.729	▼ -41%
5	.ml	177.008		305.437	▼ -42%
6	.nl	150.862		199.900	▼ -25%
7	.co.uk	130.201		228.559	▼ -43%
8	.com.br	121.371		224.770	▼ -46%
9	.ru	107.452		208.810	▼ -49%
10	.eu	102.454		125.592	▼ -18%
11	.cf	100.241		202.486	▼ -50%
12	.fr	96.208		146.638	▼ -34%
13	.co	94.947		148.134	▼ -36%
14	.in	86.044		137.891	▼ -38%
15	.gq	70.392		170.799	▼ -59%
16	.ca	70.366		123.533	▼ -43%
17	.us	61.512		-	Nova entrada
18	.sa.com	60.810		-	Nova entrada
19	.com.au	59.853		85.312	▼ -30%
20	.ch	56.669		-	Nova entrada

0 1 2 3

Top20 gTLD - novos | Top20 gTLDs - zona

Top 20 gTLDs usados em novos domínios

Posição	TLD de novo domínio	T2 2022	Barra de dados do T2	T1 2022	Mudança %
1	.com	5.750.666		6.049.245	▼ -5%
2	.xyz	503.191		11.434	▲ 4301%
3	.net	291.331		148.871	▲ 96%
4	.org	263.430		141.957	▲ 86%
5	.online	238.194		-	Nova entrada
6	.top	203.738		86.760	▲ 135%
7	.shop	172.363		82.471	▲ 109%
8	.site	145.313		-	Nova entrada
9	.info	127.696		50.469	▲ 153%
10	.store	102.916		-	Nova entrada
11	.africa	92.427		-	Nova entrada
12	.live	76.690		39.950	▲ 92%
13	.durban	60.369		-	Nova entrada
14	.buzz	51.439		66.398	▼ -23%
15	.fun	50.021		42.387	▲ 18%
16	.cyou	49.954		-	Nova entrada
17	.club	47.484		53.154	▼ -11%
18	.space	45.851		-	Nova entrada
19	.vip	41.735		14.729	▲ 183%
20	.biz	37.896		56.233	▼ -33%

Top20 gTLD - novos | Top20 gTLDs - zona

Top 20 gTLDs por % de arquivos de zonas que são novos domínios

Posição	TLD de novo domínio	T2 2022	Tamanho da zona	% da zona recém-observada	% da barra de dados da zona
1	.durban	60.369	62.683	96%	
2	.africa	92.427	140.288	66%	
3	.fun	50.021	313.557	16%	
4	.site	145.313	1.012.401	14%	
5	.store	102.916	807.924	13%	
6	.online	238.194	1.907.228	12%	
7	.live	76.690	617.500	12%	
8	.space	45.851	376.632	12%	
9	.xyz	503.191	4.295.734	12%	
10	.buzz	51.439	521.534	10%	
11	.shop	172.363	2.102.875	8%	
12	.vip	41.735	581.973	7%	
13	.cyou	49.954	783.602	6%	
14	.club	47.484	777.664	6%	
15	.top	203.738	3.491.337	6%	
16	.com	5.750.666	164.236.805	4%	
17	.info	127.696	3.748.259	3%	
18	.biz	37.896	1.439.182	3%	
19	.org	263.430	11.025.728	2%	
20	.net	291.331	13.521.180	2%	

Termos mais populares nos novos domínios

É interessante ver quantos acontecimentos do mundo real geram registros de novos domínios. As acentuadas quedas nos valores das criptomoedas afetaram claramente os registros de domínios relacionados a criptomoedas, com “crypto” saindo do Top 20 no T2.

Em abril, “ketous” manteve sua popularidade do T1, mas saiu do Top 20. Suspeitamos que esse termo esteja relacionado à popularidade da dieta Keto.

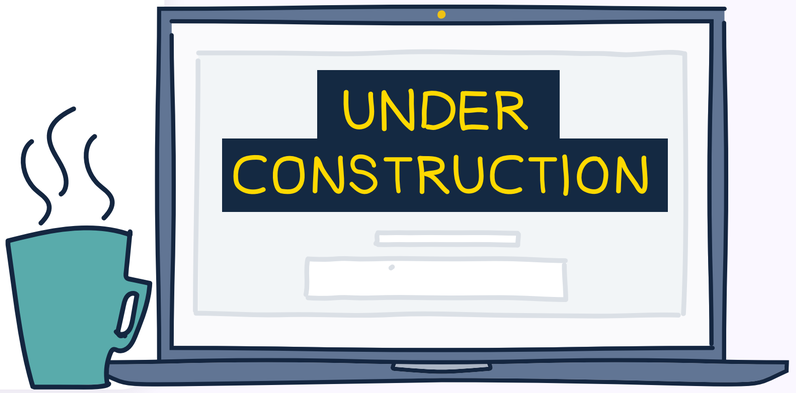
Entretanto, você pode estar se perguntando o que é “yulecheng”. É a palavra em chinês para “cassino”. Embora a China continental proíba jogos de azar de forma rigorosa, é muito mais difícil regulá-los online. Além disso, historicamente, o setor de cassinos em todo o mundo sempre teve muitos domínios associados a ele: os operadores de cassinos propagam seus negócios para muitos nomes de marcas e, consequentemente, nomes de domínios.

Quando se trata de “-ation”, temos aqui uma análise de todas as palavras no T2 que contêm o termo “-ation”:

- location **1.850**
- ration **1.925**
- formation **1.974**
- automation **2.015**
- restoration **2.104**
- corporation **2.122**
- transportation **2.274**
- renovation **2.401**
- association **2.824**
- communication **2.928**
- vacation **3.351**
- innovation **4.082**
- station **4.955**
- education **6.211**
- creation **9.680**
- foundation **11.715**
- nation **18.622**

Metodologia para os termos mais populares

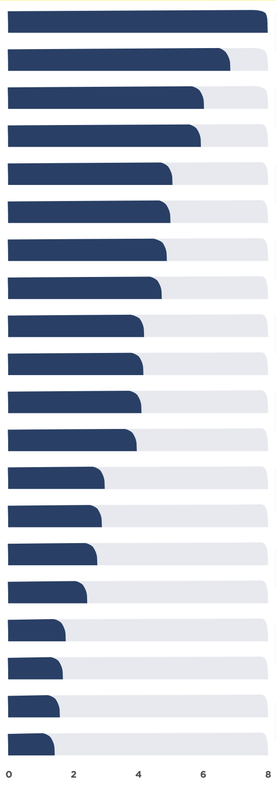
Usamos um vetorizador de texto para encontrar as strings mais comuns nos novos nomes de domínios e dividimos o total por data, o que destaca as tendências em questões de nomes de domínios. Por exemplo, vimos uma disparada nos nomes de domínios contendo “ukraine” (ucrania) após a invasão russa.



Top 20 termos mais populares... | Termos mais populares

Top 20 termos mais populares nos novos domínios

Posição	Termos mais populares do T2 2022	T2 2022	Barra de dados do T2	T1 2022	Mudança %
1	service	81.243		78.976	▲ 3%
2	ation	66.840		32.555	▲ 105%
3	online	60.351		56.439	▲ 7%
4	design	59.948		68.129	▼ -12%
5	market	48.007		41.291	▲ 16%
6	group	47.222		48.842	▼ -3%
7	solution	46.835		46.576	▲ 1%
8	studio	45.097		51.047	▼ -12%
9	health	41.723		43.491	▼ -4%
10	store	41.235		40.868	▲ 1%
11	digital	40.970		42.709	▼ -4%
12	consult	39.600		36.977	▲ 7%
13	shopping	27.301		-	Nova entrada
14	global	27.190		25.841	▲ 5%
15	yulecheng	27.079		-	Nova entrada
16	today	22.244		-	Nova entrada
17	invest	18.635		29.282	▼ -36%
18	marketing	18.166		-	Nova entrada
19	product	17.076		-	Nova entrada
20	beauty	16.169		26.479	▼ -39%



Top 20 termos mais populares... | Termos mais populares

Termos mais populares

Domínios listados | Listagens por mês

Domínios listados

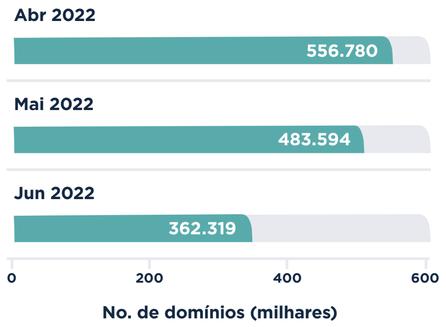
Visão geral dos domínios

Pouco mais de 1,4 milhão de domínios foram listados no último trimestre, com uma média de 468 mil por mês, o que representa uma redução de 11% em relação ao primeiro trimestre de 2022. Ainda é cedo demais para dizer se essa tendência continuará. Entretanto, duvidamos que isso ocorra — tradicionalmente, o maior número de domínios com baixa reputação é visto no segundo semestre do ano, atingindo o pico em feriados norte-americanos, como o Dia de Ação de Graças e o Natal.

- Continuamos a ver um número relativamente pequeno de operadores mal-intencionados usando um número significativo de domínios.
- Há uma clara divisão entre operadores mal-intencionados que utilizam novos nomes de domínios o mais rapidamente possível e aqueles que deixam os domínios maturar para escapar do impacto negativo à reputação proveniente de um novo domínio.
  Os tempos de maturação variam de algumas semanas a um ano.
- Alguns operadores mal-intencionados preferem comprar domínios atuais de segunda mão para explorar a boa reputação existente dos domínios. Está cada vez mais fácil comprar esses domínios antigos e maduros.

Domínios listados | Listagens por mês

Número de listagens de domínios por mês



Total do trimestre
1.402.693
▼ -11% ▼

Média mensal
467.564
▼ -57.303 ▼

O que faz com que um domínio seja listado pela Spamhaus?

Nossos sistemas avaliam centenas de sinais relacionados a um domínio e seus comportamentos associados. Os domínios são avaliados nas áreas listadas abaixo, usando várias técnicas automatizadas, que são ampliadas graças à pesquisa humana:

- Autenticação e criptografia
- Propriedade de domínios
- Sinais provenientes de tráfego em grande escala na internet
- O ambiente de hospedagem de um domínio
- Associações com spam, phishing, malware, ransomware e outras atividades fraudulentas

O mecanismo de reputação pontua um domínio; se atingir limites e condições predefinidos, ele será listado nos datasets relevantes. Esse é um processo contínuo: os domínios são avaliados e reavaliados conforme tráfego relevante é observado.

TLDs listados... | Listagem de domínios...

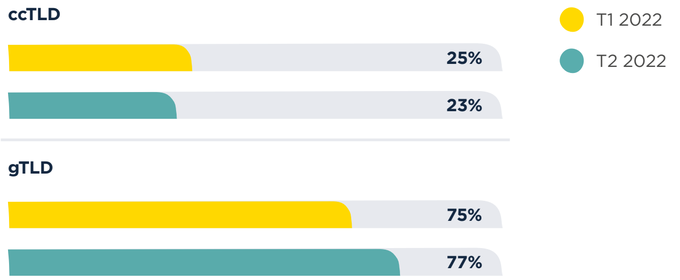
TLDs listados em nossos dados de domínios

A divisão percentual entre ccTLDs e gTLDs praticamente não mudou entre os trimestres, com os ccTLDs representando aproximadamente um quarto das listagens e os gTLDs três quartos delas.

- **.com** permanece imbatível. Muitos agentes mal-intencionados sabem que há inúmeros cenários nos quais o uso de novos nomes de gTLD mais baratos tem um impacto mais negativo em suas atividades. Afinal de contas, .com é onde a internet acontece: muito menos pessoas (e sistemas automatizados) acham suspeito se um domínio .com é usado. Junte a isso a natureza aberta desse TLD (qualquer pessoa de qualquer lugar do mundo pode comprar um .com), e não é nenhuma surpresa vê-lo como o número um na lista.
- **.cn** é o ccTLD de classificação mais alta. Continuamos vendo grandes volumes de domínios de phishing em .cn, onde alguns permanecem ativos por um longo período. Sem dúvida, a barreira idiomática contribui para o problema: é difícil para entidades fora da China relatarem os problemas às entidades chinesas. De modo inverso, é difícil para eles compreenderem os relatórios e avaliarem os casos.
- **Os TLDs Freenom** continuam tendo altos volumes de registros de uso abusivo e descartes. Mesmo com APIs antiexploração, o baixo preço (ou seja, de graça) e a facilidade de registro mantêm esses TLDs firmemente no Top 20.

TLDs listados... | Listagem de domínios...

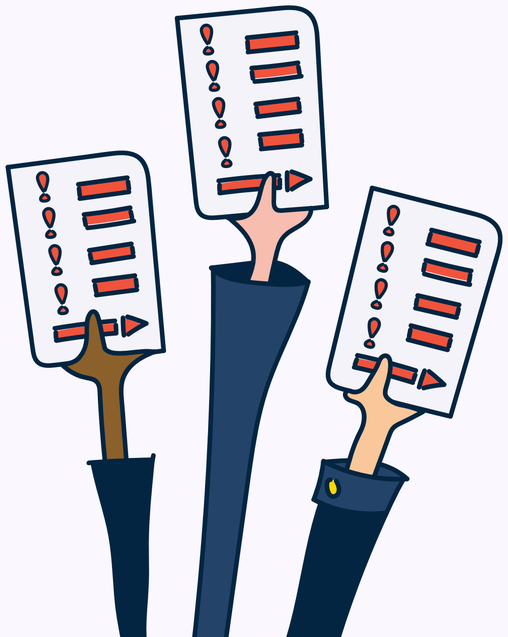
Comparação de tipos de TLDs de listagens de domínios, por trimestre



Interpretação dos dados

Registros com maior número de domínios ativos têm maior exposição ao uso abusivo. Por exemplo, no T2 2022, .net tinha mais de 13,5 milhões de domínios em sua zona, dos quais 0,39% estavam listados.

Por outro lado, .cam tinha pouco mais de 36.000 domínios em sua zona, com 17,03% deles listados em nosso dataset de domínios. Ambos estão nas nossas listas dos Top 20. Ainda assim, um tinha um percentual muito maior de domínios ativos listados do que o outro.



Top 20 TLDs... | Listagens por...

Top 20 TLDs listados

Posição	TLD de domínio	Tipo de TLD	T2 2022	Barra de dados do T2	T1 2022	Mudança %
1	.com	gTLD	675.968		700.932	▽ -4%
2	.cn	ccTLD	128.017		199.895	▽ -36%
3	.info	gTLD	58.334		42.643	△ 37%
4	.net	gTLD	53.282		61.793	▽ -14%
5	.top	gTLD	40.720		40.742	— 0%
6	.xyz	gTLD	37.658		34.714	△ 8%
7	.tk	ccTLD	29.337		26.234	△ 12%
8	.org	gTLD	21.198		19.647	△ 8%
9	.live	gTLD	20.680		23.013	▽ -10%
10	.ml	ccTLD	19.353		16.142	△ 20%
11	.biz	gTLD	17.250		25.056	▽ -31%
12	.bar	gTLD	15.272		-	Nova entrada
13	.ru	ccTLD	15.033		20.305	▽ -26%
14	.ga	ccTLD	15.021		13.002	△ 16%
15	.cf	ccTLD	14.519		11.811	△ 23%
16	.uk	ccTLD	13.039		15.440	▽ -16%
17	.us	ccTLD	12.793		19.026	▽ -33%
18	.online	gTLD	12.421		12.611	▽ -2%
19	.gq	ccTLD	11.596		-	Nova entrada
20	.in	ccTLD	10.346		-	Nova entrada

0 200 400 600 800

Top 20 TLDs... | Listagens por...

Listagens por Top 20 ccTLDs

Posição	TLD de domínio	T2 2022	Barra de dados do T2	T1 2022	Mudança %
1	.cn	128.017		199.895	▽ -36%
2	.tk	29.337		26.234	△ 12%
3	.ml	19.353		16.142	△ 20%
4	.ru	15.033		20.305	▽ -26%
5	.ga	15.021		13.002	△ 16%
6	.cf	14.519		11.811	△ 23%
7	.uk	13.039		15.440	▽ -16%
8	.us	12.793		19.026	▽ -33%
9	.gq	11.596		9.946	△ 17%
10	.in	10.346		8.736	△ 18%
11	.co	7.647		8.617	▽ -11%
12	.cc	6.816		4.490	△ 52%
13	.me	4.359		3.625	△ 20%
14	.pw	2.987		2.139	△ 40%
15	.eu	2.970		3.657	▽ -19%
16	.ng	2.677		1.643	△ 63%
17	.de	2.295		2.073	△ 11%
18	.ci	1.619		-	Nova entrada
19	.ir	1.615		-	Nova entrada
20	.br	1.479		-	Nova entrada

0 50 100 150

Top 20 gTLDs... | Top 20 gTLD...

Top 20 gTLDs usados em listagens de domínios

Posição	TLD de domínio	T2 2022	Barra de dados do T2	T1 2022	Mudança %
1	.com	675.968		700.932	▽ -4%
2	.info	58.334		42.643	△ 37%
3	.net	53.282		61.793	▽ -14%
4	.top	40.720		40.742	— 0%
5	.xyz	37.658		34.714	△ 8%
6	.org	21.198		19.647	△ 8%
7	.live	20.680		23.013	▽ -10%
8	.biz	17.250		25.056	▽ -31%
9	.bar	15.272		11.122	△ 37%
10	.online	12.421		12.611	▽ -2%
11	.shop	10.205		7.736	△ 32%
12	.work	9.197		51.709	▽ -82%
13	.club	7.810		6.064	△ 29%
14	.site	6.196		7.161	▽ -13%
15	.cam	6.176		-	Nova entrada
16	.icu	5.929		26.698	▽ -78%
17	.click	4.339		-	Nova entrada
18	.store	4.118		5.224	▽ -21%
19	.buzz	3.874		16.764	▽ -77%
20	.tokyo	3.484		-	Nova entrada

0 200 400 600 800

Top 20 gTLDs... | Top 20 gTLD...

Top 20 gTLDs por % de arquivos de zonas com listagens de domínios

Posição	TLD de domínio	T2 2022	Tamanho da zona	% da zona listado	% da barra de dados da zona
1	.cam	6.176	36.269	17,03%	
2	.bar	15.272	260.041	5,87%	
3	.work	9.197	266.056	3,46%	
4	.live	20.680	617.500	3,35%	
5	.click	4.339	160.003	2,71%	
6	.info	58.334	3.748.259	1,56%	
7	.biz	17.250	1.439.182	1,20%	
8	.top	40.720	3.491.337	1,17%	
9	.club	7.810	777.664	1,00%	
10	.xyz	37.658	4.295.734	0,88%	
11	.buzz	3.874	521.534	0,74	
12	.tokyo	3.484	497.501	0,70%	
13	.online	12.421	1.907.228	0,65%	
14	.site	6.196	1.012.401	0,61%	
15	.icu	5.929	1.093.330	0,54%	
16	.store	4.118	807.924	0,51%	
17	.shop	10.205	2.102.875	0,49%	
18	.com	675.968	164.236.805	0,41%	
19	.net	53.282	13.521.180	0,39%	
20	.org	21.198	11.025.728	0,19%	

0% 5% 10% 15% 20%

Termos de phishing mais populares nas listagens de domínios

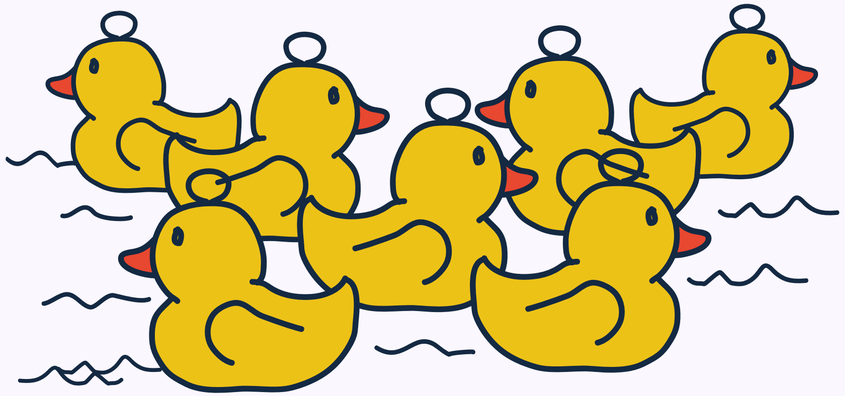
Na parte superior da tabela (novamente) está “amazon” como o principal termo e nome de marca usado em domínios de phishing. Enquanto isso, “apple” teve um aumento de 104% em popularidade para campanhas de phishing, tendo sido superado apenas por “icloud”, com uma elevação de 133%. Entretanto, um termo de marca saiu do Top 20 no T2: “fedex”.

Quando se trata de domínios de phishing, os pesquisadores da Spamhaus veem regularmente agentes mal-intencionados usando uma “chamada à ação” no nome de domínio. O Top 20 reflete isso com o aparecimento de palavras como “verify” (verifique), “review” (revise) e “update” (atualize). Neste trimestre, vimos “bank” entrar diretamente na quarta posição, com “info” não muito distante, na sétima.

Que termos os agentes mal-intencionados usam para nomes de domínios?

Alguns falsários não se importam com a aparência de um nome de domínio; outros, sim — e esses últimos preferem uma das duas opções:

1. Tentar parecer uma marca legítima, com a inclusão de um nome de marca muito conhecido, p.ex.: “amazon”.
2. Usar palavras no nome de domínio que pareçam uma chamada à ação, p.ex.: “update now” (atualize agora) e “verify your account” (verifique sua conta).



Top 20 termos de phishing... | Termos de phishing

Top 20 termos de phishing nas listagens de domínios

Posição	Termo	T2 2022	Barra de dados do T2	T1 2022	Mudança %
1	amazon	9.759		6.460	▲ 51%
2	secure	9.460		6.068	▲ 56%
3	support	6.995		4.514	▲ 55%
4	bank	6.740		-	Nova entrada
5	account	6.518		3.985	▲ 64%
6	online	6.251		3.966	▲ 58%
7	info	6.174		-	Nova entrada
8	service	4.785		2.740	▲ 75%
9	verify	4.474		2.639	▲ 70%
10	verification	4.368		2.781	▲ 57%
11	icloud	4.018		1.724	▲ 133%
12	apple	3.971		1.949	▲ 104%
13	security	3.620		2.156	▲ 68%
14	session	3.069		-	Nova entrada
15	review	2.727		-	Nova entrada
16	update	2.444		1.542	▲ 58%
17	wallet	2.416		3.505	▼ -31%
18	findmy	2.134		-	Nova entrada
19	view	1.937		-	Nova entrada
20	payment	1.910		-	Nova entrada

Top 20 termos de phishing... | Termos de phishing

Termos de phishing

Tipos de listagens

No T2, parece que quando se trata do tipo de uso abusivo de domínios comprometidos, o phishing foi a escolha do trimestre, com um aumento de 81%, enquanto o uso abusivo de botnet CC diminuiu 60%.

Para domínios comprometidos que apresentam comportamento malicioso, lembre-se de algumas coisas:

- A grande maioria desses comprometimentos ocorre por meios automatizados, e as máquinas não se importam com o TLD associado.
- Muitos sites comprometidos recebem o "presente" de um Sistema de Distribuição de Tráfego (TDS). Eles permitem que os agentes mal-intencionados girem conteúdo, URLs e geoblocking. Nossos pesquisadores veem centenas de URLs únicos para alguns sites, alguns dos quais estão ativos há meses.
- Atualmente, a maioria dos comprometimentos que observamos estão no nível de site. Nesses casos, um Sistema de Gerenciamento de Conteúdo (CMS), como o WordPress ou Drupal, normalmente contém uma falha explorável que é usada para inserir arquivos ou código maliciosos no site. Os agentes mal-intencionados a usam para obter domínios "gratuitos" com (quase sempre) uma boa reputação existente, o oposto de comprar um domínio novíssimo sem reputação. O bônus é que esses domínios não serão derrubados, já que seus proprietários são legítimos.
- Em poucos casos, vemos comprometimentos em nível de DNS. Eles normalmente ocorrem por meio de credenciais de registradores roubadas ou, às vezes, por meio de painéis de administração roubados ou hackeados, como o cPanel ou Plesk. Após o controle do DNS autoritativo estar nas mãos de agentes mal-intencionados, é fácil para eles adicionarem nomes de host que possam apontar para uma infraestrutura própria. Novamente, o benefício aqui é que domínios existentes com uma boa reputação estão sendo usados para finalidades ruins.

Diferenças entre domínios comprometidos e maliciosos

Um **domínio comprometido** é aquele no qual fica evidente para nossa equipe de pesquisa que o domínio tem um proprietário legítimo; entretanto, um agente mal-intencionado o comprometeu. Um exemplo é quando um Sistema de Gerenciamento de Conteúdo (CMS) é hackeado, e o domínio está sendo usado para enviar spam, resultando na listagem do domínio. Dentro da Spamhaus, esses tipos de listagens são chamados de "explorados-legítimos".

Um **domínio malicioso** é aquele em que o domínio é registrado pela pessoa que comete o uso abusivo na internet.

Tipos de listagens

Tipos de listagens

Baixa reputação

Maliciosos	Comprometidos
969.475	12.715
▼ -16% ▼	▼ -22% ▼

A pontuação da reputação de um domínio excedeu os limites da política.

Botnet CC

Maliciosos	Comprometidos
4.773	57
▼ -25% ▼	▼ -60% ▼

Um domínio é registrado para uso para um comando e controle (CC) de botnet.
(Um subconjunto de baixa reputação.)

Malware

Maliciosos	Comprometidos
6.278	4.400
▲ 55% ▲	▼ -6% ▼

Um domínio que se observou ser utilizado na distribuição de malware.
(Um subconjunto de baixa reputação.)

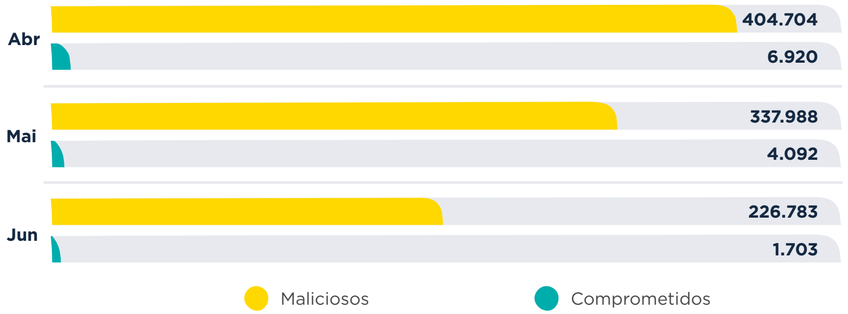
Phishing

Maliciosos	Comprometidos
278.341	14.630
▲ 6% ▲	▲ 81% ▲

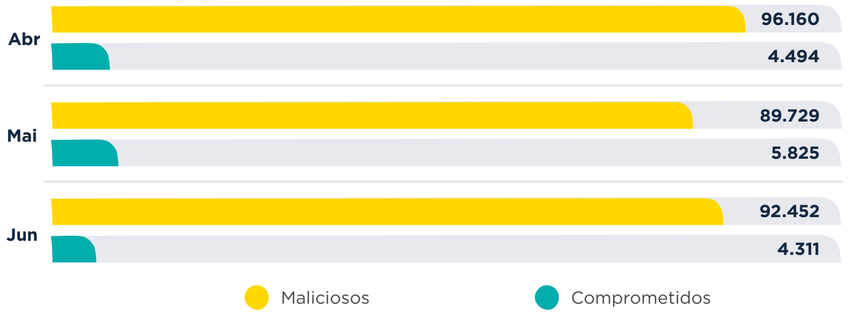
Um domínio associado a atividades de phishing.
(Um subconjunto de baixa reputação.)

Tipos de uso abusivo

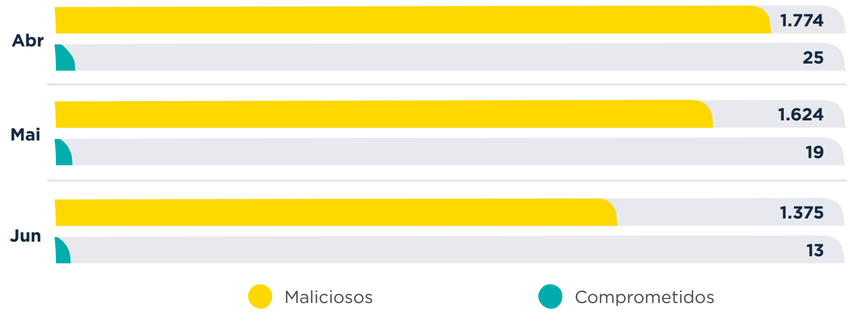
Baixa reputação por mês



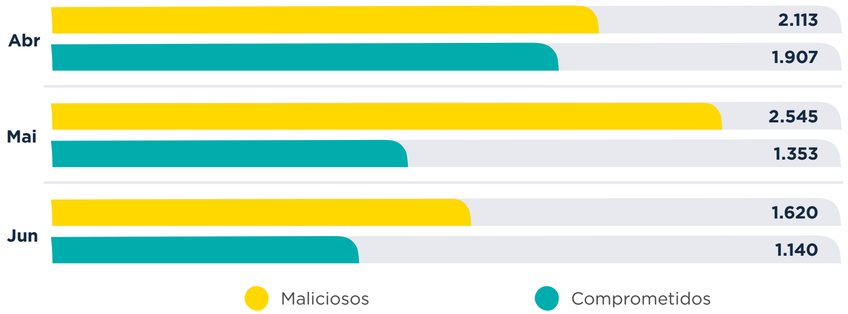
Phishing por mês



Botnet CC por mês



Malware por mês



Recomendar...

Recomendações do trimestre

Já que este é o primeiro relatório publicado, começaremos com algumas recomendações genéricas em relação à reputação de nomes de domínio para proprietários de domínios. Nem todas elas se aplicarão a todos, e algumas podem parecer genéricas, mas é bom ter essas coisas em mente ao tomar decisões que envolvem seus nomes de domínio.

- **Se você controla seu nome de domínio, certifique-se de que isso não mude.** Tenha uma combinação forte e exclusiva de login/senha para o gerenciamento do nome de domínio e adicione a 2FA a isso.
- **Hospedar seu nome de domínio em uma rede questionável pode refletir mal em sua reputação.** Assim como uma empresa contribui para a característica da vizinhança, a característica da vizinhança também se reflete na empresa. Lembre-se de que os domínios funcionam da mesma forma!
- **O anonimato não contribui para uma boa reputação.** Se uma empresa tem um nome de domínio, certifique-se de que ele esteja visível no WHOIS/RDAP. Mesmo que um nome de empresa não seja um PII, muitos registradores ainda o filtrarão.
- **Menos é mais quando pensamos na quantidade de nomes de domínio que você usa.** Ao comprar nomes de domínio adicionais, sempre se pergunte se o uso de um subdomínio de seu nome de domínio primário é melhor. Costuma ser. Se você realmente precisar de nomes de domínio diferentes, certifique-se de que eles possam ser facilmente vinculados ao nome de domínio primário e sempre considere o impacto à reputação causado por um novo nome de domínio nos e-mails, SEOs e expectativas dos clientes/do público. Um novo domínio que se pareça demais com seu domínio existente pode ser relatado como phishing!

Informações adicionais

Sobre a Spamhaus

A Spamhaus é a autoridade confiável em reputação de IPs e domínios, posicionada de forma exclusiva no setor devido à sua sólida ética, imparcialidade e qualidade dos dados acionáveis. Esses dados não apenas protegem, mas também proporcionam insights de redes e e-mails em todo o mundo.

Com mais de duas décadas de experiência, nossos pesquisadores e caçadores de ameaças se concentram em expor atividade maliciosa para tornar a internet um local melhor para todos. Uma grande variedade de setores, incluindo as principais empresas globais de tecnologia, utiliza os dados da Spamhaus. Atualmente, ela protege mais de três bilhões de caixas de correio em todo o mundo.

Metodologia do relatório

- Várias fontes, incluindo ISPs, ESPs, empresas e especialistas em pesquisa, compartilham dados com a Spamhaus. Esses dados são analisados por nossos pesquisadores por meio de machine learning, heurística e investigações manuais para identificar comportamentos maliciosos e baixas reputações. Os dados nesse relatório refletem os domínios maliciosos que a Spamhaus observou, identificou e listou. Eles não refletem todos os domínios maliciosos e de baixa reputação que existem na internet.
- As campanhas maliciosas são direcionadas regularmente para localizações geográficas, ISPs ou organizações específicas. Isso, por sua vez, pode distorcer os números.
- Devido a problemas contínuos que fogem ao nosso controle relacionados a dados da WHOIS e RDAP, alguns de nossos dados estão incompletos. Esse é um resultado direto da GDPR.
- Onde houver dados de arquivos de zonas ausentes, agradeceríamos se os registradores entrassem em contato conosco e compartilhassem tais dados.