Actualización trimestral sobre reputación de dominios de Spamhaus

T2 2022

Spamhaus, líder independiente en reputación de IP y dominios, revisa la ecosfera de los nombres de dominio. Desde el número de dominios registrados recientemente hasta el nivel de abuso que observan nuestros investigadores, esta actualización destaca las tendencias, ofrece información sobre la mala reputación de los dominios y ayuda a los proveedores a introducir mejoras.

Bienvenido a la Actualización trimestral sobre reputación de dominios de Spamhaus: T2 2022.

Entrar

Índice

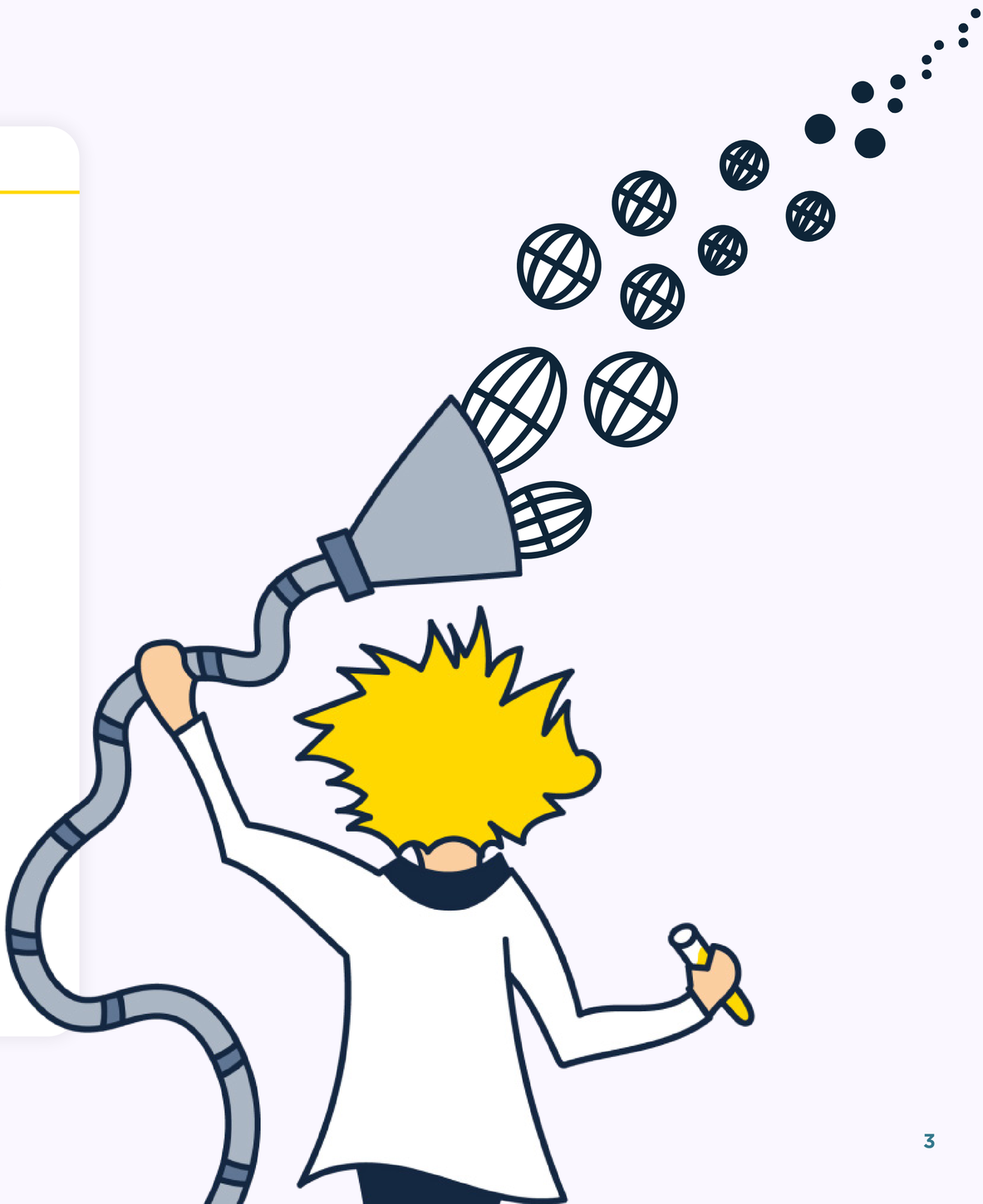
Visión general

¿Por qué analizamos los dominios y su reputación asociada? ¿Por qué tiene sentido utilizar un nombre de dominio como marcador de reputación para filtrar decisiones, ya sea que dichas decisiones estén relacionadas con el tráfico general de Internet, correos electrónicos o malware?

Los dominios tienen una “forma” previsible, por lo que pueden extraerse y actuar sobre ellos con facilidad. Numerosos tipos de software de seguridad admiten el uso de dominios (o nombres de servidor) para destacar problemas e informar las decisiones. Esto no es ninguna sorpresa, puesto que el sistema de nombres de dominio (DNS) es fundamental para casi todo lo que sucede en Internet y forma su núcleo, “los registros de recursos almacenados en el DNS asocian los nombres de dominio con otros tipos de información” (https://es.wikipedia.org/wiki/Domain_Name_System).

No importa lo que hagas en Internet, sea legal o no, (casi siempre) necesitas usar un nombre de dominio. Sin un nombre de dominio, no podrían realizarse la mayoría de las actividades maliciosas ni mucho menos tener éxito.

Visión general (continuación)



Visión general (cont.)

Piensa en estos escenarios:

- Una campaña de phishing por SMS utiliza un nombre de dominio corto adquirido específicamente (es decir, un registro malicioso) para dirigir a los destinatarios directos hacia un portal de pago falso. Elimina o filtra el dominio y será imposible realizar el fraude.
- Un malware intenta crear un canal de comando y control usando un nombre de dominio malicioso para contactar con el servidor que utiliza un individuo poco confiable. Retira el dominio y no será posible establecer la comunicación.
- Un correo electrónico de spam relacionado con medicamentos falsos se envía con todos los protocolos configurados correctamente en el mensaje (SPF, DKIM y DMARC). Incluso aunque todos superen la comprobación, saber que el dominio es malicioso emitirá una señal de alerta y el correo electrónico se tratará de manera diferente.

Los individuos poco confiables con experiencia necesitan nombres de dominio para cometer abusos, es así de sencillo. Algunos necesitan cientos de dominios para evitar filtros de mala reputación y blocklists; otros solo necesitan unos cuantos proveedores de servicios cuidadosamente seleccionados que no suelan retirar dominios con rapidez.

Queremos hacer hincapié en este tipo de actividad maliciosa y destacar a los proveedores de servicios que van más lejos para asegurarse de no ofrecer ningún refugio seguro a los individuos poco confiables. A medida que publiquemos más informes, esperamos seguir aportando contenidos para proporcionar más contexto e información adicional sobre el mundo de la reputación de dominios.

Dominios nuevos | Número de nuevos...

Dominios nuevos

Visión general de los nuevos dominios

Se registraron un total de 15,3 millones de nuevos dominios el último trimestre, con una media mensual de 5,1 millones. Esto supone una importante reducción del 43% frente al T1 de este año, cuando observamos 25,6 millones de nuevos dominios.

Mayo fue el mes más activo, con 5,6 millones de dominios; no obstante, los tres meses estuvieron cerca de la media mensual del trimestre, con escasas variaciones.

Es importante señalar que un nuevo dominio no es un domino malicioso en sí. Sin embargo, un considerable número de abusos están relacionados con nuevos nombres de dominio. Una razón es que si un individuo poco confiables adquiere un nuevo dominio y lo usa inmediatamente, es prácticamente imposible que los sistemas y profesionales de seguridad estén al tanto de la existencia de dicho dominio. Por desgracia, solo se descubre su existencia una vez que se inicia la campaña maliciosa. Además, al usar nuevos dominios, los individuos poco confiables evitan que los registros y registradores realicen retiradas preventivas.

Dominios nuevos | Número de nuevos...

Número de nuevos dominios por mes

Total trimestral

15 253 514

▼-43%▼

Media mensual

5 084 505

▼-3 764 414▼

¿Qué es un dominio nuevo?

Spamhaus clasifica un “nuevo dominio” como uno que ha sido registrado u observado recientemente por Spamhaus e incluido durante un plazo de 24 horas en su dataset Zero Reputation Domain (ZRD). Los dominios recién creados no suelen utilizarse para fines legítimos durante las primeras 24 horas después de su registro; por otra parte, los cibercriminales registran y queman cientos de dominios cada día. Cuando estos nuevos dominios se utilizan de inmediato, es un fuerte indicador de posible comportamiento malicioso.

El equipo de investigación crea esta lista a partir de varias fuentes de datos, como archivos de zona y datos de Passive DNS y SMTP compartidos por los registradores. Por lo tanto, los datos de nuevos dominios no reflejan el número exacto de nuevos dominios, sino el número de nuevos dominios con visibilidad para Spamhaus.

Dominios nuevos... | Tipos de TLD...

Dominios nuevos por dominio de nivel superior (TLD)

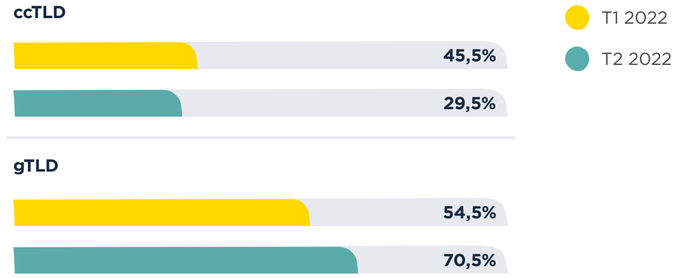
Todos los TLD que salieron de la lista de los 20 primeros TLD en el T2 eran ccTLD. Teniendo esto en cuenta, no será ninguna sorpresa descubrir que los ccTLD bajaron más del 15% en el T2 cuando se revise la cuota por tipos de TLD.

También observarás que algunos gTLD experimentaron un gran aumento en el número de nuevos dominios en sus zonas en comparación con el trimestre anterior. Por ejemplo, .xyz tuvo un enorme aumento del 4301 %. En algunos casos, podemos relacionar el aumento de la popularidad de algunos dominios de gTLD con promociones ofrecidas por el TLD. Los registradores pueden ofrecer estas promociones en todos sus registros o solo en algunos seleccionados.

Como la mayoría de estas promociones reducen considerablemente el precio (¡no es raro un descuento del 90%!), permiten adquirir muchos más nombres de dominio por la misma cantidad de dinero. Esto resulta muy atractivo no solo para los especuladores de nombres de dominio, sino también para los individuos poco confiables que queman infinidad de dominios como parte de su “modelo de negocio”.

Dominios nuevos... | Tipos de TLD...

Comparación de tipos de TLD de nuevos dominios: intertrimestral



Dominios de nivel superior (TLD): una explicación rápida

Hay un par de dominios de nivel superior (TLD) diferentes que incluyen:

- **TLD genéricos (gTLD)**: se encuentran bajo la jurisdicción de la ICANN. Algunos gTLD son abiertos, es decir, cualquiera puede utilizarlos, como .com, otros tienen políticas estrictas que regulan quién y cómo pueden usarse, como .bank, y otros están cerrados, como .honda.
- **Dominios territoriales (ccTLD)**: normalmente están relacionados con un país o una región. Los registradores definen las políticas relacionadas con estos TLD; algunos permiten registros desde cualquier lugar, otros requieren presencia local y algunos venden todo su nombre de espacios a otros.

Los 20 primeros TLD... | Los 20 primeros ccTLD...

Los 20 TLD más usados en nuevos dominios

Clasificación	TLD nuevos dominios	Tipo de TLD	T2 2022	Barra de datos del T2	T1 2022	% de cambio
1	.com	gTLD	5 750 666		6 049 245	▼ -5%
2	.xyz	gTLD	503 191		-	Nueva 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		-	Nueva entrada
8	.tk	ccTLD	228 359		660 463	▼ -65%
9	.top	gTLD	203 738		-	Nueva entrada
10	.ga	ccTLD	183 826		312 729	▼ -41%
11	.ml	ccTLD	177 008		305 437	▼ -42%
12	.shop	gTLD	172 363		-	Nueva entrada
13	.nl	ccTLD	150 862		199 900	▼ -25%
14	.site	gTLD	145 313		-	Nueva entrada
15	.co.uk	ccTLD	130 201		228 559	▼ -43%
16	.info	gTLD	127 696		-	Nueva entrada
17	.com.br	ccTLD	121 371		224 770	▼ -46%
18	.ru	ccTLD	107 452		208 810	▼ -49%
19	.store	gTLD	102 916		-	Nueva entrada
20	.eu	ccTLD	102 454		125 592	▼ -18%

Los 20 primeros TLD... | Los 20 primeros ccTLD...

Los 20 ccTLD más usados en nuevos dominios

Clasificación	TLD nuevos dominios	T2 2022	Barra de datos del T2	T1 2022	% de cambio
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		-	Nueva entrada
18	.sa.com	60 810		-	Nueva entrada
19	.com.au	59 853		85 312	▼ -30%
20	.ch	56 669		-	Nueva entrada

Los 20 primeros gTLD: nuevos | Los 20 primeros gTLD: zonas

Los 20 gTLD más usados en nuevos dominios

Clasificación	TLD nuevos dominios	T2 2022	Barra de datos del T2	T1 2022	% de cambio
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		-	Nueva entrada
6	.top	203 738		86 760	▲ 135%
7	.shop	172 363		82 471	▲ 109%
8	.site	145 313		-	Nueva entrada
9	.info	127 696		50 469	▲ 153%
10	.store	102 916		-	Nueva entrada
11	.africa	92 427		-	Nueva entrada
12	.live	76 690		39 950	▲ 92%
13	.durban	60 369		-	Nueva entrada
14	.buzz	51 439		66 398	▼ -23%
15	.fun	50 021		42 387	▲ 18%
16	.cyou	49 954		-	Nueva entrada
17	.club	47 484		53 154	▼ -11%
18	.space	45 851		-	Nueva entrada
19	.vip	41 735		14 729	▲ 183%
20	.biz	37 896		56 233	▼ -33%

Los 20 primeros gTLD: nuevos | Los 20 primeros gTLD: zonas

Los 20 primeros gTLD por % de archivo de zona que son nuevos dominios

Clasificación	TLD nuevos dominios	T2 2022	Tamaño de zona	% de zona recién observado	Barra de datos de % de 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%	

Tendencias de términos en los nuevos dominios

Resulta interesante comprobar hasta qué punto los cambios en el mundo real impulsan el registro de nuevos dominios. Los importantes descensos en el valor de las criptomonedas han afectado claramente el registro de dominios relacionados con estas monedas y el término “crypto” ha desaparecido de la lista de los 20 primeros en el T2.

En abril, “ketous” continuó su popularidad desde el T1, pero salió también de la lista de los 20 primeros. Sospechamos que este término está relacionado con la popularidad de la dieta cetógena.

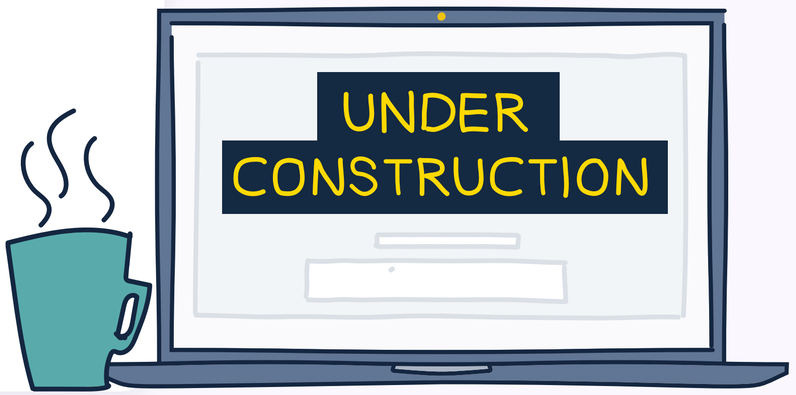
Mientras tanto, tal vez te preguntes qué significa “yulecheng”. Significa “casino” en chino.
Si bien el juego está estrictamente prohibido en China continental, el juego online resulta mucho más difícil de regular. Además, históricamente, el sector de los casinos siempre ha tenido un gran número de dominios relacionado con ellos: los operadores de casinos expanden su negocio mediante muchos nombres de marca y, por lo tanto, nombres de dominio.

En cuanto a “ation”, aquí tienes desglosados todos los términos utilizados en el T2 que terminan en “-ation”:

- location **1850**
- ration **1925**
- formation **1974**
- automation **2015**
- restoration **2104**
- corporation **2122**
- transportation **2274**
- renovation **2401**
- association **2824**
- communication **2928**
- vacation **3351**
- innovation **4082**
- station **4955**
- education **6211**
- creation **9680**
- foundation **11 715**
- nation **18 622**

Metodología para las tendencias de términos

Utilizamos un vectorizador de textos para averiguar las cadenas más comunes en los nuevos nombres de dominio y desglosar su número por fecha, lo que muestra las tendencias temáticas en los nombres de dominio. Por ejemplo, observamos un aumento en los nombres de dominio que contienen “ukraine” después de la invasión rusa.



Las 20 principales tendencias de términos en nuevos dominios

Clasificación	Tendencias de términos T2 2022	T2 2022	Barra de datos del T2	T1 2022	% de cambio
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		-	Nueva entrada
14	global	27 190		25 841	▲ 5%
15	yulecheng	27 079		-	Nueva entrada
16	today	22 244		-	Nueva entrada
17	invest	18 635		29 282	▼ -36%
18	marketing	18 166		-	Nueva entrada
19	product	17 076		-	Nueva entrada
20	beauty	16 169		26 479	▼ -39%

Tendencias de términos

Dominios incluidos | Inclusiones por mes

Dominios incluidos

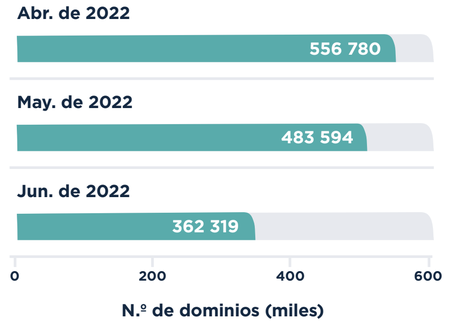
Visión general de dominios

Durante el último trimestre se incluyeron algo más de 1,4 millones de dominios, con una media de 468 000 por mes. Esto supone una reducción del 11% en comparación con el T1 de 2022. Es demasiado pronto para saber si esta tendencia continuará. Sin embargo, es poco probable; tradicionalmente, el mayor número de dominios con mala reputación surgen en la segunda mitad del año, con máximas alrededor de las vacaciones estadounidenses como Acción de gracias y Navidad.

- Seguimos viendo un número relativamente pequeño de operadores maliciosos que utilizan un gran número de dominios.
- Existe una clara separación entre los operadores maliciosos que utilizan los nuevos dominios lo antes posible y quienes dejan envejecer los dominios para evitar el impacto reputacional negativo de un nuevo dominio. Los tiempos de envejecimiento van desde algunas semanas hasta más de un año.
- Algunos operadores maliciosos prefieren comprar dominios existentes de segunda mano para explotar la buena reputación de los dominios existentes. La posibilidad de comprar estos dominios viejos y envejecidos es cada vez más fácil.

Dominios incluidos | Inclusiones por mes

Número de inclusiones de dominios por mes



Total trimestral

1 402 693

▼ -11% ▼

Media mensual

467 564

▼ -57 303 ▼

¿Qué motiva la inclusión de un dominio por parte de Spamhaus?

Nuestros sistemas evalúan cientos de señales relacionadas con un dominio y sus comportamientos asociados. Los dominios se evalúan en relación con las áreas que se indican a continuación, usando varias técnicas automáticas reforzadas con investigación humana:

- Autenticación y cifrado
- Propietario del dominio
- Señales de tráfico de Internet a gran escala
- Entorno de alojamiento de un dominio
- Asociaciones con spam, phishing, malware, ransomware y otras actividades fraudulentas

El motor de reputación analiza un dominio; si cumple las condiciones y los umbrales predeterminados, se incluye en los datasets relevantes. Es un proceso continuo: los dominios se evalúan y revalúan a medida que se observa el tráfico relevante.

TLD incluidos... | Dominios incluidos...

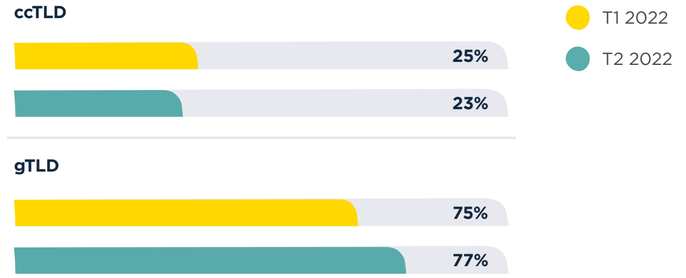
TLD incluidos en nuestros datos de dominio

La cuota porcentual entre ccTLD y gTLD apenas varió de un trimestre al otro, pues los ccTLD representaron aproximadamente una cuarta parte de las inclusiones y los gTLD las otras tres restantes.

- **.com** mantiene el liderazgo. Muchos individuos poco confiables saben que existen numerosos escenarios en los cuales el hecho usar nombres de gTLD nuevos y económicos tiene un impacto más adverso sobre sus actividades. Al fin y al cabo, .com es la columna vertebral de Internet; a muchas menos personas (y sistemas automáticos) les parece sospechoso si se utiliza un dominio .com. Si esto se combina con la naturaleza abierta de este TLD (cualquiera puede comprar un .com), no sorprende que ocupe la primera posición de la lista.
- **.cn** es el primer ccTLD. Seguimos encontrando un gran número de dominios de phishing en .cn, donde algunos permanecen activos durante mucho tiempo. Sin duda, la barrera lingüística contribuye a este problema: a las entidades situadas fuera de China les resulta difícil denunciar los problemas a las entidades chinas. Por su parte, a estas les resulta complicado comprender los informes y evaluar los casos.
- **Los TLD Freenom** siguen experimentando elevados volúmenes de registros abusivos y desechables. Incluso con API antiabuso, el bajo precio (básicamente gratis) y la facilidad de registro motivan que estos TLD se mantengan con firmeza entre los 20 primeros.

TLD incluidos... | Dominios incluidos...

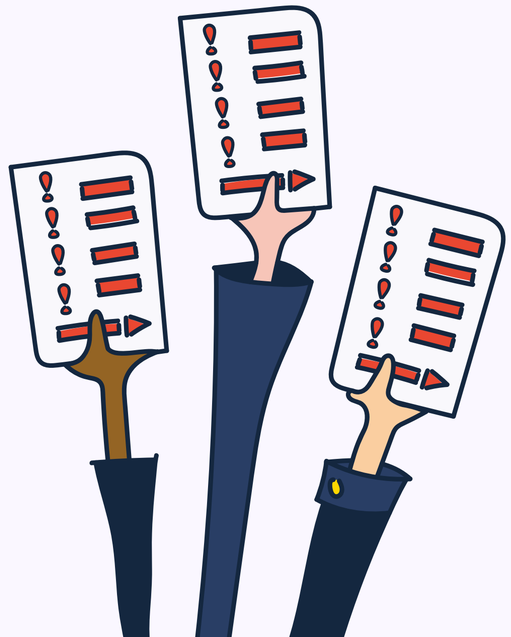
Comparación de tipos de TLD en los dominios: intertrimestral



Interpretación de los datos

Los registros con un mayor número de dominios activos están más expuestos a posibles abusos. Por ejemplo, en el T2 de 2022 .net tenía más de 13,5 millones de dominios en su zona, de los cuales un 0,39% estaban incluidos.

Entre tanto, .cam tenía poco más de 36 000 dominios en su zona, con el 17,03% incluidos en nuestro dataset de dominios. Ambos se encuentran entre las 20 posiciones principales de nuestra clasificación. Uno de ellos tenía un porcentaje de dominios activos incluidos muy superior al otro.



Los 20 primeros TLD... | Inclusiones por...

Los 20 primeros TLD incluidos

Clasificación	TLD de dominio	Tipo de TLD	T2 2022	Barra de datos del T2	T1 2022	% de cambio
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		-	Nueva 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		-	Nueva entrada
20	.in	ccTLD	10 346		-	Nueva entrada

0 200 400 600 800

Los 20 primeros TLD... | Inclusiones por...

Inclusiones según los 20 primeros ccTLD

Clasificación	TLD de dominio	T2 2022	Barra de datos del T2	T1 2022	% de cambio
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		9946	17%
10	.in	10 346		8736	18%
11	.co	7647		8617	-11%
12	.cc	6816		4490	52%
13	.me	4359		3625	20%
14	.pw	2987		2139	40%
15	.eu	2970		3657	-19%
16	.ng	2677		1643	63%
17	.de	2295		2073	11%
18	.ci	1619		-	Nueva entrada
19	.ir	1615		-	Nueva entrada
20	.br	1479		-	Nueva entrada

0 50 100 150

Los 20 primeros gTLD... | Los 20 primeros gTLD...

Los 20 primeros gTLD usados en dominios incluidos

Clasificación	TLD de dominio	T2 2022	Barra de datos del T2	T1 2022	% de cambio
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		7736	32%
12	.work	9197		51 709	-82%
13	.club	7810		6064	29%
14	.site	6196		7161	-13%
15	.cam	6176		-	Nueva entrada
16	.icu	5929		26 698	-78%
17	.click	4339		-	Nueva entrada
18	.store	4118		5224	-21%
19	.buzz	3874		16 764	-77%
20	.tokyo	3484		-	Nueva entrada

Los 20 primeros gTLD... | Los 20 primeros gTLD...

Los 20 primeros gTLD por % de archivo de zona con dominios incluidos

Clasificación	TLD de dominio	T2 2022	Tamaño de zona	% de zona incluida	Barra de datos de % de zona
1	.cam	6176	36 269	17,03%	
2	.bar	15 272	260 041	5,87%	
3	.work	9197	266 056	3,46%	
4	.live	20 680	617 500	3,35%	
5	.click	4339	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	7810	777 664	1,00%	
10	.xyz	37 658	4 295 734	0,88%	
11	.buzz	3874	521 534	0,74%	
12	.tokyo	3484	497 501	0,70%	
13	.online	12 421	1 907 228	0,65%	
14	.site	6196	1 012 401	0,61%	
15	.icu	5929	1 093 330	0,54%	
16	.store	4118	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%	

Tendencias de términos de phishing en dominios incluidos

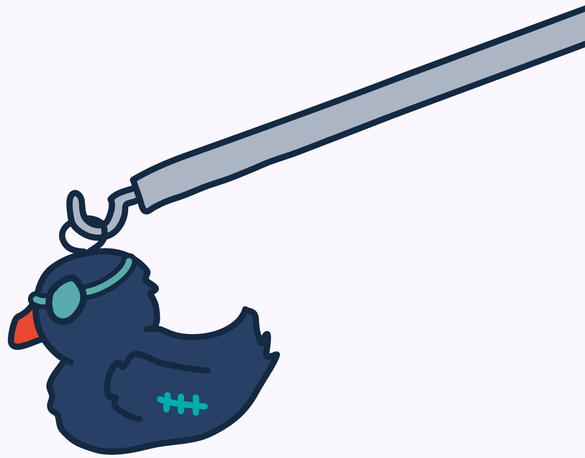
En la primera posición de la tabla (de nuevo) está “amazon” como término y marca más usados en dominios de phishing. Entre tanto, “apple” aumentó un 104% su popularidad para campañas de phishing, pero fue superado por “icloud” con un aumento del 133%. No obstante, hay un término de marca que abandonó la lista de 20 primeros en el T2: “fedex”.

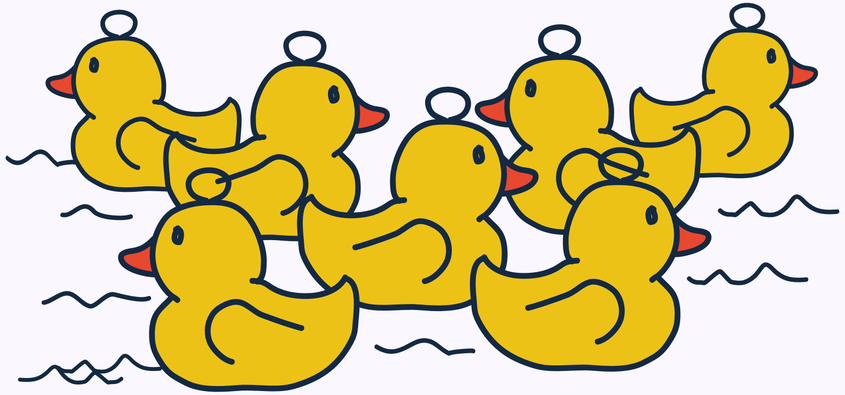
En cuanto a los dominios de phishing, los investigadores de Spamhaus observan regularmente que los individuos poco confiables utilizan una “call to action” en el nombre de dominio. Esto se refleja en la lista de los 20 primeros, donde aparecen palabras como “verify”, “review” y “update”. Este trimestre, el término “bank” se incorporó directamente en el n.º 4, seguido poco después por “info” en el n.º 7.

¿Qué términos utilizan los individuos poco confiables en sus nombres de dominio?

Algunos individuos no se preocupan por el aspecto del dominio, pero otros sí. Estos últimos suelen preferir una de estas dos opciones:

1. Intentan asemejarse a una marca legítima añadiendo un nombre de marca conocido, como “amazon”.
2. Utilizan palabras en el nombre de dominio que emitan una llamada a la acción, como “update now” o “verify your account”.

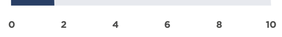




20 primeros términos de phishing... | Términos de phishing

Los 20 primeros términos de phishing en dominios incluidos

Clasificación	Término	T2 2022	Barra de datos del T2	T1 2022	% de cambio
1	amazon	9759		6460	▲ 51%
2	secure	9460		6068	▲ 56%
3	support	6995		4514	▲ 55%
4	bank	6740		-	Nueva entrada
5	account	6518		3985	▲ 64%
6	online	6251		3966	▲ 58%
7	info	6174		-	Nueva entrada
8	service	4785		2740	▲ 75%
9	verify	4474		2639	▲ 70%
10	verification	4368		2781	▲ 57%
11	icloud	4018		1724	▲ 133%
12	apple	3971		1949	▲ 104%
13	security	3620		2156	▲ 68%
14	session	3069		-	Nueva entrada
15	review	2727		-	Nueva entrada
16	update	2444		1542	▲ 58%
17	wallet	2416		3505	▼ -31%
18	findmy	2134		-	Nueva entrada
19	view	1937		-	Nueva entrada
20	payment	1910		-	Nueva entrada



20 primeros términos de phishing... | Términos de phishing

Términos de phishing

Tipos de inclusiones

En el T2, parece que en términos del tipo de abuso de los dominios comprometidos, el phishing fue el más popular este trimestre, con un aumento del 81%, mientras que el abuso de botnet C&C descendió un 60%.

Para los dominios comprometidos que presentan un comportamiento malicioso, hay que tener en cuenta algunas cosas:

- La gran mayoría de estos compromisos se realizan usando medios automáticos y las máquinas no se preocupan por el TLD asociado.
- Muchos sitios web comprometidos reciben como "regalo" un sistema de distribución de tráfico (TDS), que permite a los individuos poco confiables rotar los contenidos, las URL y el bloqueo geográfico. Nuestros investigadores detectan cientos de URL únicas de muchos sitios, algunas de las cuales llevan activas varios meses.
- Actualmente, la mayoría de los compromisos que observamos se producen al nivel del sitio web. En estos casos, un sistema de gestión de contenidos (CMS) como WordPress o Drupal normalmente contiene una vulnerabilidad explotable que se utiliza para insertar archivos o código malicioso en el sitio web. Los individuos poco confiables utilizan estas vulnerabilidades para obtener dominios "gratis" existentes con (casi siempre) buena reputación, lo contrario de adquirir un dominio nuevo sin reputación. La ventaja añadida es que estos dominios no serán retirados, puesto que sus propietarios son legítimos.
- En algunos casos, encontramos compromisos al nivel del DNS. Normalmente se producen mediante el robo de las credenciales del registrador o, en ocasiones, el robo o jaqueo de paneles de administración, como cPanel o Plesk. Cuando los individuos poco confiables tienen en sus manos el control de los DNS acreditados, les resulta sencillo añadir nombres de servidor que apunten hacia su propia infraestructura. De nuevo, la ventaja estriba en que se utilizan dominios existentes con buena reputación para fines maliciosos.

Diferencias entre dominios comprometidos y maliciosos

Un **dominio comprometido** es uno donde es evidente para nuestro equipo de investigadores que el dominio tiene un propietario legítimo, pero lo comprometió un individuo poco confiable. Un ejemplo es cuando se jaquea un sistema de gestión de contenidos (CMS) y el dominio se utiliza para enviar spam, lo que motiva la inclusión del dominio. En Spamhaus, nos referimos a este tipo de inclusiones como "legítimo abusado".

Un **dominio malicioso** es aquel registrado por la persona que comete el abuso de Internet.

Tipos de inclusiones

Tipos de inclusiones

Mala reputación

Malicioso	Comprometido
969 475	12 715
▼ -16% ▼	▼ -22% ▼

La puntuación de reputación del dominio superó los límites de la política.

Botnet C&C

Malicioso	Comprometido
4773	57
▼ -25% ▼	▼ -60% ▼

Se registra un dominio para ser usado por un botnet de comando y control (C&C). (Un subconjunto de mala reputación).

Malware

Malicioso	Comprometido
6278	4400
▲ 55% ▲	▼ -6% ▼

Se observa que un dominio se utiliza en la distribución de malware. (Un subconjunto de mala reputación).

Phishing

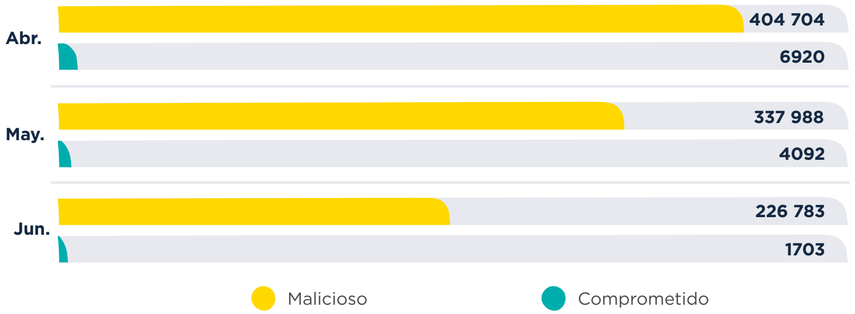
Malicioso	Comprometido
278 341	14 630
▲ 6% ▲	▲ 81% ▲

Un dominio está relacionado con actividades de phishing. (Un subconjunto de mala reputación).

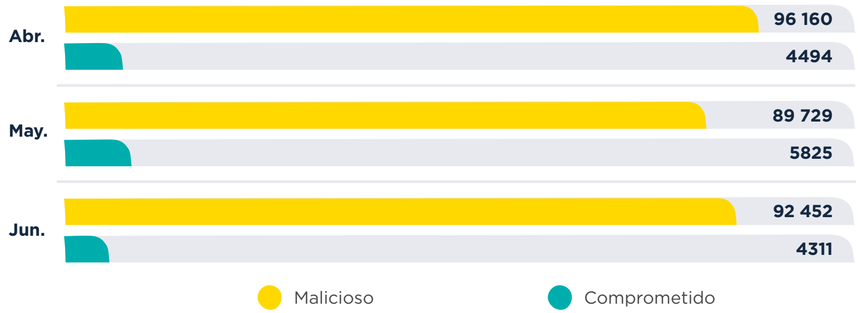
Tipos de abuso

Tipos de abuso

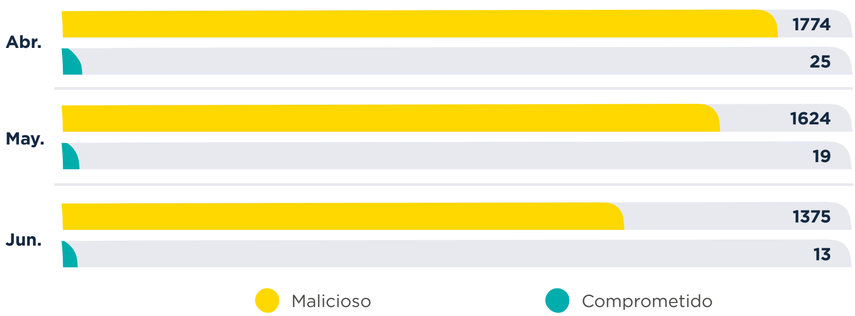
Mala reputación por mes



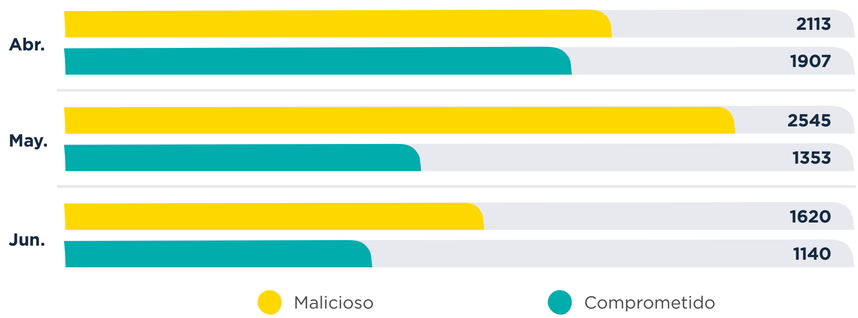
Phishing por mes



Botnet C&C por mes



Malware por mes



Recomendaciones del trimestre

Como es el primer informe que publicamos, empezaremos con algunas recomendaciones generales sobre la reputación de los nombres de dominio para los propietarios. No todas ellas serán válidas para todos y algunas pueden parecer algo generales, pero es buena idea tenerlas en cuenta al tomar decisiones relacionadas con los nombres de dominio.

- **Si controlas tu nombre de dominio, asegúrate de que siga así.** Elige una combinación robusta y única de usuario/contraseña para gestionar el nombre de dominio y añade 2FA para obtener mayor seguridad.
- **Alojar tu nombre de dominio en una red cuestionable podría afectar negativamente su reputación.** Al igual que un negocio influye en el carácter del vecindario, el carácter del vecindario se refleja en el negocio. ¡Recuerda que los dominios funcionan de la misma manera!
- **El anonimato no contribuye a una buena reputación.** Si el nombre de dominio es propiedad de una empresa/negocio, asegúrate de que sea visible en WHOIS/RDAP. Aunque el nombre de la empresa no es información de identificación personal, muchos registradores siguen filtrándolo.
- **Menos es más en cuanto al número de nombres de dominio que utilices.** Cuando compres más nombres de dominio, pregúntate siempre si no sería mejor utilizar un subdominio en tu nombre de dominio principal. A menudo es mejor. Si realmente necesitas nuevos nombres de dominio, asegúrate de que puedan vincularse fácilmente con el principal y ten siempre en cuenta el impacto reputacional de un nuevo nombre de dominio en el correo electrónico, la SEO y las expectativas de los clientes/público objetivo. ¡Un dominio nuevo que se parezca mucho a tu dominio actual podría denunciarse como phishing!

Información adicional

Acerca de Spamhaus

Spamhaus, la autoridad de confianza en reputación de dominios e IP, se encuentra en una posición única en el sector debido a su sólida ética, imparcialidad y calidad de sus datos. Estos datos no solo protegen sino que también suministran información sobre las redes y el correo electrónico en todo el mundo.

Con más de dos décadas de experiencia, nuestros investigadores y especialistas en amenazas se dedican a exponer la actividad maliciosa para convertir Internet en un lugar mejor para todos. Los datos de Spamhaus se utilizan en un gran número de sectores, incluidas las principales empresas tecnológicas del mundo. Actualmente, protegen más de 3 mil millones de buzones de correo en todo el mundo.

Metodología de informe

- Varias fuentes, como ISP, ESP, empresas y especialistas en investigación comparten datos con Spamhaus. Nuestros investigadores analizan estos datos mediante machine learning, heurística e investigaciones manuales para identificar comportamientos maliciosos y mala reputación. Los datos que contiene este informe reflejan los dominios maliciosos que Spamhaus ha observado, identificado e incluido, y no reflejan todos los dominios maliciosos y con mala reputación que se encuentran en Internet.
- Las campañas maliciosas se dirigen periódicamente a territorios, ISP y organizaciones específicas. Esto puede introducir sesgos en los datos.
- Debido a cuestiones actuales fuera de nuestro control en relación con los datos de WHOIS y RDAP, algunos de nuestros datos no están completos. Es un resultado directo del RGPD.
- Cuando carecemos de datos del archivo de zona, agradecemos que los registradores se comuniquen y compartan estos datos con nosotros.