

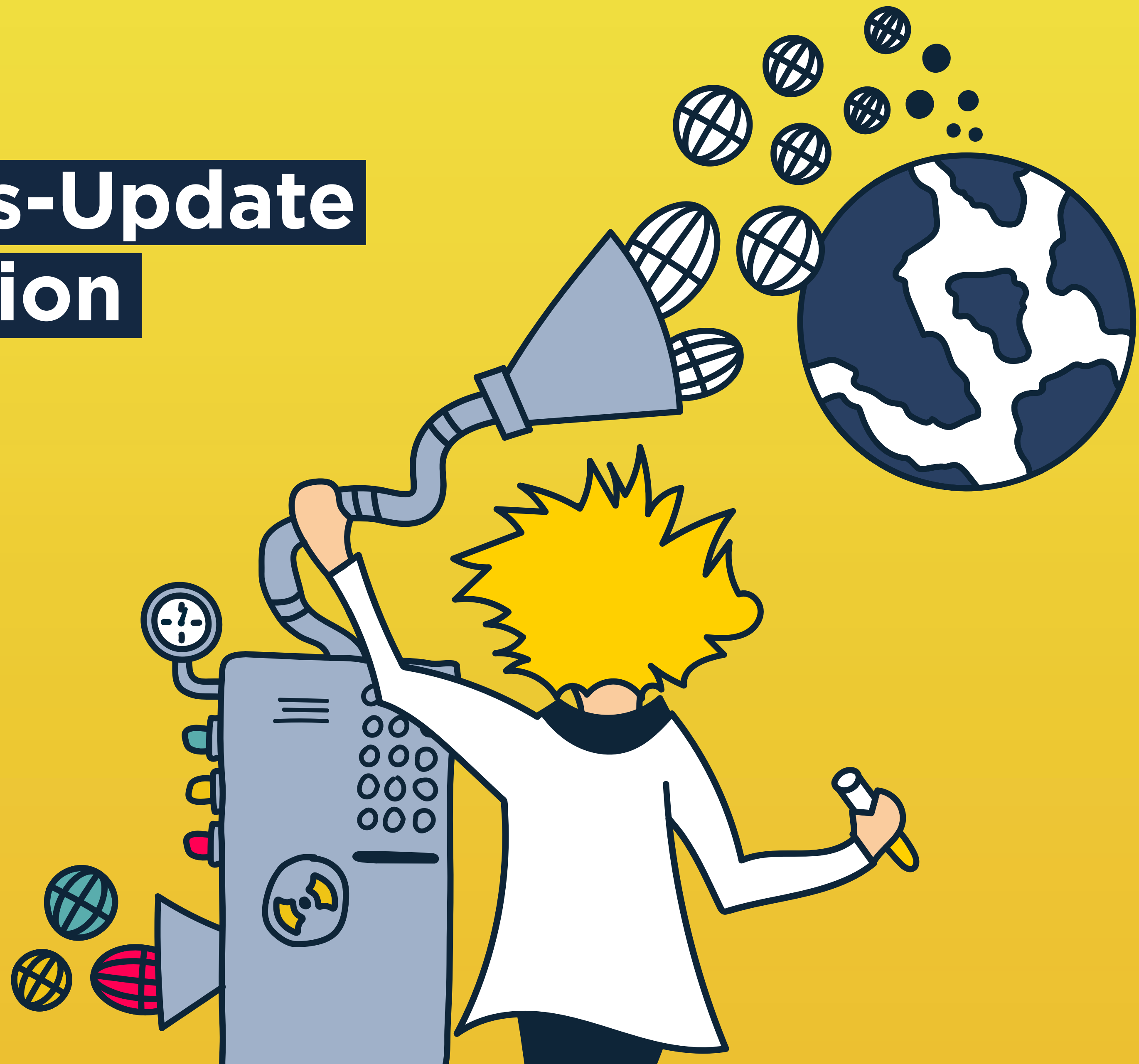
Spamhaus – Quartals-Update zur Domain-Reputation

Q2-2022

Als führendes Unternehmen für IP- und Domain-Reputation überprüft Spamhaus auch das Ökosystem der Domain Names. Ob neu registrierte Domains oder missbrauchte bestehende Domains: Unser Update beleuchtet Trends, liefert Informationen über Domains mit schlechter Reputation und hebt Anbieter hervor, bei denen positive Entwicklungen zu beobachten sind.

Herzlich willkommen beim Quartals-Update zur Domain-Reputation von Spamhaus für das 2. Quartal 2022.

Mehr



Inhalt

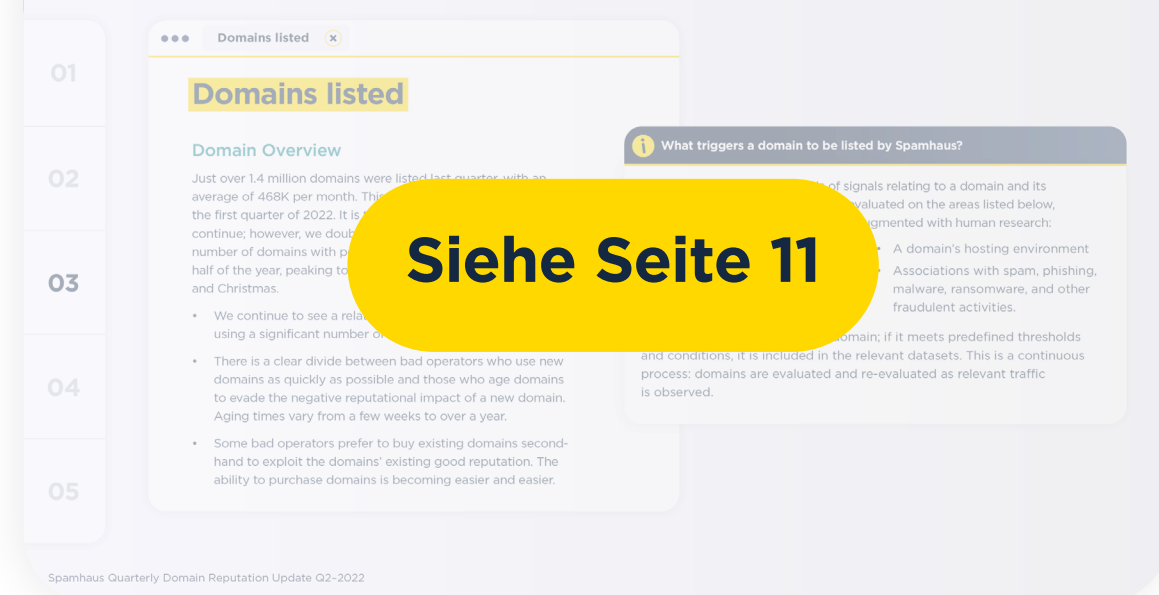
Überblick



Neue Domains



Gelistete Domains



Unsere Quartalsempfehlungen



Weitere Informationen



01

02

03

04

05



Überblick



Überblick

Warum betrachten wir Domains und ihre Reputation? Warum ist es sinnvoll, beim Filtern einen Domain Name als Reputationskennzeichen zu nutzen, sei es für E-Mail, Malware oder allgemeinen Internetverkehr?

Da Domains eine vorhersehbare Form haben, ist es einfach, sie zu extrahieren und darauf zu reagieren. Viele Arten von Sicherheitssoftware nutzen Domains (oder Hostnamen) zur Problemerkennung und als Entscheidungsgrundlage. Das überrascht nicht, spielt doch das Domain Name System (DNS) eine zentrale Rolle für fast alles im Internet. In seinem Innern „verknüpfen die im DNS enthaltenen Ressourcen Domain Names mit anderen Arten von Informationen“

(nach https://en.wikipedia.org/wiki/Domain_Name_System).

Unabhängig von der Art der Aktivität im Internet (ob legitim oder nicht) muss man fast immer einen Domain Name verwenden. Ohne Domain Name würden die meisten bösartigen Aktivitäten bereits im Keim erstickt, ohne Chance auf Erfolg.

Überblick
(Fortsetzung)



01

02

03

04

05



Überblick (S. 2)

Betrachten Sie diese Szenarien:

- Mit einem nur für die bösartige Registrierung gekauften kurzen Domain Name lockt eine SMS-Phishing-Kampagne die Empfänger auf ein betrügerisches Zahlungsportal. Wird die Domain gelöscht oder herausgefiltert, wird der Betrug unterbunden.
- Über Malware soll ein Command&Control-Kanal erstellt werden. Dafür wird über einen bösartigen Domain Name die Verbindung zu einem vom Angreifer betriebenen Server hergestellt. Wird die Domain abgeschaltet, erfolgt keine Kommunikation.
- Eine gefälschte Spam-E-Mail für Medikamente wird versendet. Alle Authentifizierungsprotokolle sind korrekt eingestellt (SPF, DKIM, DMARC). Sollte die E-Mail durchgehen, wird sie im Wissen, dass es sich um eine bösartige Domain handelt, trotzdem markiert und entsprechend behandelt.

Selbst gerissene Angreifer brauchen Domain Names für ihre Angriffe – so einfach ist das. Manche brauchen Hunderte von Domains, um Blocklists zu umgehen und ihre schlechte Reputation zu verbergen. Andere hingegen brauchen nur wenige, sorgfältig ausgewählte Dienstleister, die vielleicht nicht schnell genug reagieren.

Wir beleuchten diese Art bösartiger Aktivitäten und heben auch Dienstleister hervor, die besonders bemüht sind, Angreifern keine Plattform zu bieten. Mit aktuellen Berichten wollen wir Ihnen informative Inhalte, zusätzlichen Kontext und bessere Einblicke in die Welt der Domain-Reputation geben.



01

02

03

04

05

●●● Neue Domains x Anzahl neuer ... x

Neue Domains

Neue Domains im Überblick

Insgesamt wurden im vergangenen Quartal 15,3 Millionen neue Domains registriert, im Durchschnitt 5,1 Millionen pro Monat. Dies sind 43 % weniger als im 1. Quartal, als noch 25,6 Millionen neue Domains verzeichnet wurden.

Der Mai war mit 5,6 Millionen Domains der stärkste Monat. Allerdings lagen alle drei Monate nahe am Durchschnitt, mit geringen Abweichungen.

Dabei ist eine neue Domain nicht zwangsläufig auch eine schlechte Domain. Trotzdem wird ein erheblicher Anteil bössartiger Aktivitäten mit neuen Domain Names assoziiert. Wenn ein Angreifer eine neue Domain erwirbt und diese sofort nutzt, ist die Wahrscheinlichkeit gering, dass Sicherheitssysteme und -experten schnell genug reagieren. Die Existenz wird häufig leider erst dann erkannt, wenn die bössartige Kampagne schon begonnen hat. Durch die Nutzung neuer Domains hindern Angreifer Registrierungsstellen auch daran, sie vorbeugend vom Netz zu nehmen.

●●● Neue Domains x Anzahl neuer ... x

Anzahl neuer Domains pro Monat

April 2022

4.490.369

Mai 2022

5.589.977

Juni 2022

5.173.168

Anzahl neuer Domains (Mio.)

Gesamt im Quartal

15.253.514

▼-43 %▼

Monatsdurchschnitt

5.084.505

▼-3.764.414▼



Was ist eine neue Domain?

Spamhaus stuft eine Domain als „neue Domain“ ein, wenn sie neu registriert oder neu beobachtet wurde, und nimmt sie für 24 Stunden in seinen Datensatz der Zero Reputation Domains (ZRD) auf. Neu registrierte Domains werden nur selten innerhalb der ersten 24 Stunden zu legitimen Zwecken genutzt. Cyberkriminelle wiederum registrieren und „verbrennen“ täglich Hunderte von Domains. Tauchen solche neuen Domains in der Praxis auf, ist das ein starkes Indiz für potenziell bössartige Aktivitäten.

Das Rechercheteam nutzt für diese Liste Datenquellen wie Passive DNS, SMTP-Daten und Zonendateien, die von den Registrierungsstellen bekannt gegeben werden. Die neuen Domain-Daten entsprechen daher nicht der genauen Zahl neuer Domains, sondern der Anzahl der neuen Domains, die für Spamhaus sichtbar sind.

01

02

03

04

05

● ● ● Neue Domains ... x TLD-Typen ... x

Neue Domains nach Top Level Domains (TLD)

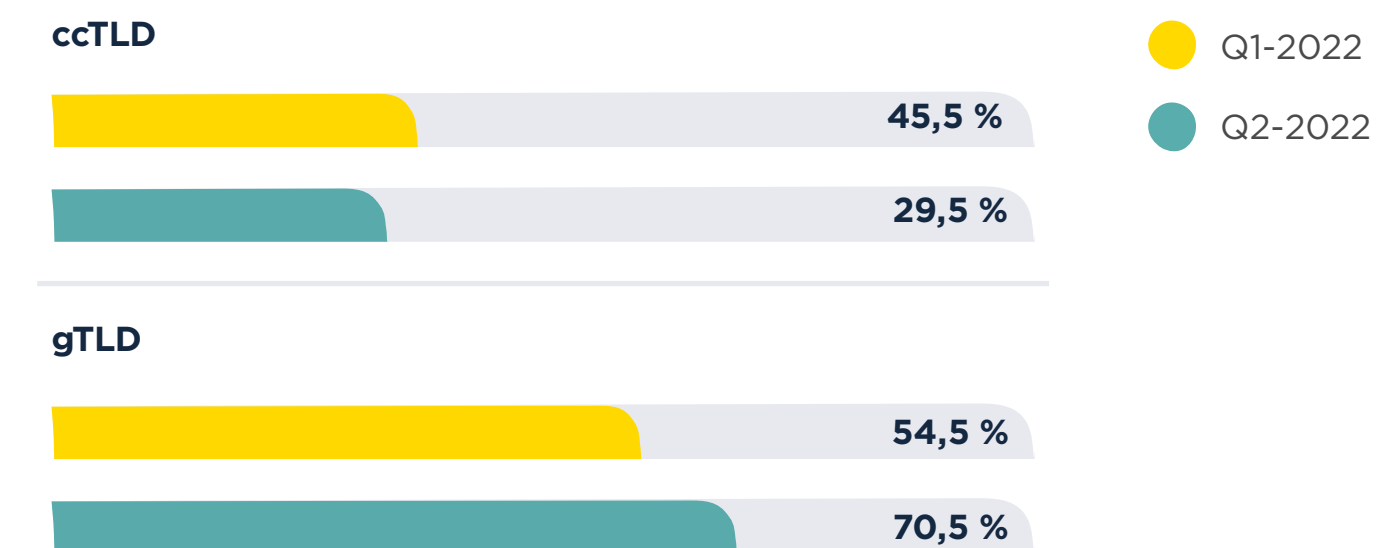
Alle im 2. Quartal aus den Top 20 gefallenen TLDs waren ccTLDs. Daher überrascht es nicht, dass der Anteil der ccTLDs gegenüber dem vorigen Quartal um mehr als 15 % gesunken ist.

Bei einigen gTLDs hat die Anzahl neuer Domains in ihren Zonen gegenüber dem vorigen Quartal deutlich zugenommen. So verzeichnete .xyz beispielsweise satte 4301 % an Zuwachs. In einigen Fällen ist die zunehmende Beliebtheit der gTLDs-Domains auf Werbeaktionen der TLD zurückzuführen. Registrierungsstellen führen solche Aktionen übergreifend oder nur für ausgewählte Bereiche durch.

Da die meisten dieser Werbeaktionen mit drastischen Preissenkungen (bis zu 90 %) einhergehen, kann ein Anmelder für denselben Betrag viel mehr Domain Names erwerben. Das ist nicht nur für Domain-Name-Spekulanten höchst attraktiv, sondern auch für Angreifer, die im Rahmen ihres „Geschäftsmodells“ ungezählte Domains verbrennen.

● ● ● Neue Domains ... x TLD-Typen ... x

Vergleich neuer Domain-TLD-Typen gegenüber dem vorigen Quartal



i Top Level Domains kurz erklärt

Es gibt eine Reihe verschiedener Top Level Domains (TLDs), beispielsweise:

- **Generische TLDs (gTLDs)** – diese fallen in den Verantwortungsbereich der ICANN. Manche gTLDs sind offen, d. h., sie können von jedem genutzt werden. Bei anderen wird hingegen durch strikte Richtlinien reguliert, wer sie wie nutzen darf, z. B. .bank, und wieder andere sind geschlossen wie z. B. .honda.
- **Länderspezifische TLDs (ccTLDs)** – diese beziehen sich in der Regel auf ein Land bzw. eine Region. Die Registrierungsstellen legen Richtlinien für diese TLDs fest. Einige lassen Registrierungen von überall zu, andere fordern eine lokale Präsenz, und noch andere vergeben Lizenzen für ihren Namensraum.

01

02

03

04

05

Die in neuen Domains verwendeten
Top 20 TLDs

Rang	Neue TLD	TLD-Typ	Q2-2022	Q2-Daten	Q1-2022	% Veränderung
1	.com	gTLD	5.750.666		6.049.245	▼ -5 %
2	.xyz	gTLD	503.191		-	Neuzugang
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		-	Neuzugang
8	.tk	ccTLD	228.359		660.463	▼ -65%
9	.top	gTLD	203.738		-	Neuzugang
10	.ga	ccTLD	183.826		312.729	▼ -41 %
11	.ml	ccTLD	177.008		305.437	▼ -42 %
12	.shop	gTLD	172.363		-	Neuzugang
13	.nl	ccTLD	150.862		199.900	▼ -25 %
14	.site	gTLD	145.313		-	Neuzugang
15	.co.uk	ccTLD	130.201		228.559	▼ -43 %
16	.info	gTLD	127.696		-	Neuzugang
17	.com.br	ccTLD	121.371		224.770	▼ -46 %
18	.ru	ccTLD	107.452		208.810	▼ -49 %
19	.store	gTLD	102.916		-	Neuzugang
20	.eu	ccTLD	102.454		125.592	▼ -18 %

Die in neuen Domains verwendeten
Top 20 ccTLDs

Rang	Neue TLD	Q2-2022	Q2-Daten	Q1-2022	% Veränderung
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		-	Neuzugang
18	.sa.com	60.810		-	Neuzugang
19	.com.au	59.853		85.312	▼ -30 %
20	.ch	56.669		-	Neuzugang

01

02

03

04

05

Die in neuen Domains verwendeten
Top 20 gTLDs

Rang	Neue TLD	Q2-2022	Q2-Daten	Q1-2022	% Veränderung
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		-	Neuzugang
6	.top	203.738		86.760	▲ 135 %
7	.shop	172.363		82.471	▲ 109 %
8	.site	145.313		-	Neuzugang
9	.info	127.696		50.469	▲ 153 %
10	.store	102.916		-	Neuzugang
11	.africa	92.427		-	Neuzugang
12	.live	76.690		39.950	▲ 92 %
13	.durban	60.369		-	Neuzugang
14	.buzz	51.439		66.398	▼ -23 %
15	.fun	50.021		42.387	▲ 18 %
16	.cyou	49.954		-	Neuzugang
17	.club	47.484		53.154	▼ -11 %
18	.space	45.851		-	Neuzugang
19	.vip	41.735		14.729	▲ 183 %
20	.biz	37.896		56.233	▼ -33 %

0246

Die neuen Top 20 gTLDs nach %
der Zonendateien

Rang	Neue TLD	Q2-2022	Zonengröße	% der Zone, neu beobachtet	% der Zonendaten
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 %	

025%50%75%100%

01

● ● ● Trendbegriffe ... ✕

Trendbegriffe bei neuen Domains

Es ist interessant, wie viele Entwicklungen aus der realen Welt Registrierungen neuer Domains auslösen. Der starke Wertrückgang bei den Kryptowährungen hat sich deutlich auf die entsprechenden Domain-Registrierungen ausgewirkt. So ist „crypto“ im 2. Quartal nicht mehr in den Top 20 vertreten.

Im April war „ketous“ zwar noch so beliebt wie im 1. Quartal, fiel dann jedoch aus den Top 20 heraus. Wir vermuten hier einen Zusammenhang mit der Popularität der Keto-Diät.

Gleichzeitig fragen Sie sich vielleicht, was „yulecheng“ ist. „Yulecheng“ ist Chinesisch für „Casino“. Während Glücksspiele in China eigentlich streng verboten sind, ist dies online viel schwieriger zu regulieren. Schon immer hatten weltweit viele Domains mit der Glücksspielbranche zu tun. Casinos betreiben ihre Geschäfte unter vielen Markennamen und damit auch unter vielen Domain Names.

Hier haben wir für Sie eine Liste aller Wörter aus dem 2. Quartal mit dem Bestandteil „ation“ zusammengestellt:

- 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**

Methodik für Trendbegriffe ✕

Mit einem Textvektorisierer suchen wir die gängigsten Zeichenfolgen in neuen Domain Names und schlüsseln diese nach Datum auf. So erkennen wir Trends bei den Themen der Domain Names. Nach der russischen Invasion war beispielsweise ein drastischer Anstieg bei Domain Names mit dem Bestandteil „ukraine“ zu verzeichnen.



04

05

01

02

03

04

05

Die Top 20 der Trendbegriffe in neuen Domains

Rang	Trendbegriffe Q2-2022	Q2-2022	Q2-Daten	Q1-2022	% Veränderung
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		-	Neuzugang
14	global	27.190		25.841	▲ 5 %
15	yulecheng	27.079		-	Neuzugang
16	today	22.244		-	Neuzugang
17	invest	18.635		29.282	▼ -36 %
18	marketing	18.166		-	Neuzugang
19	product	17.076		-	Neuzugang
20	beauty	16.169		26.479	▼ -39 %

Trendbegriffe



01



Gelistete Domains



Einträge pro Monat



Gelistete Domains

Domains im Überblick

Im vergangenen Quartal wurden gut 1,4 Millionen Domains gelistet. Der Monatsdurchschnitt lag bei 468.000. Dies war eine Verringerung um 11 % gegenüber dem 1. Quartal 2022. Es ist noch nicht abzusehen, ob der Trend sich fortsetzen wird. Das bezweifeln wir jedoch. Normalerweise tauchen die meisten Domains mit schlechter Reputation im zweiten Halbjahr auf. Die Höchstwerte werden zu den amerikanischen Feiertagen Thanksgiving und Weihnachten erreicht.

- Wir sehen weiterhin eine relativ kleine Anzahl zwielichtiger Betreiber, die eine beträchtliche Anzahl von Domains nutzen.
- Es gibt eine klare Linie zwischen zwielichtigen Betreibern, die neue Domains so schnell wie möglich nutzen, und solchen, die neue Domains erst „altern“ lassen, um die neuen Domains anhaftende schlechte Reputation zu umgehen. Die Alterungszeit variiert von wenigen Wochen bis zu mehr als einem Jahr.
- Manche zwielichtige Betreiber ziehen es vor, bestehende Domains aus zweiter Hand zu kaufen, um den guten Ruf einer Domain auszunutzen. Der Kauf alter und gealterter Domains wird außerdem immer einfacher.

02

03

04

05



Gelistete Domains

Einträge pro Monat



Domain-Einträge pro Monat

April 2022

556.780

Mai 2022

483.594

Juni 2022

362.319

0 200 400 600

Anzahl Domains (in Tausend)

Gesamt im Quartal

1.402.693

▼-11 %▼

Monatsdurchschnitt

467.564

▼-57.303▼



Was führt dazu, dass eine Domain von Spamhaus gelistet wird?

Unsere Systeme bewerten Hunderte von Signalen, die sich auf eine Domain und deren Verhalten beziehen. Domains werden mithilfe automatisierter Techniken anhand der folgenden Punkte bewertet und von menschlichen Rechterspezialisten begutachtet:

- Authentifizierung und Verschlüsselung
- Eigentümer der Domain
- Hinweise auf starken Internetverkehr
- Hosting-Umgebung der Domain
- Verbindungen zu Spam, Phishing, Malware, Ransomware und anderen betrügerischen Aktivitäten.

Die Reputationsmaschine errechnet eine Punktzahl für die Domain. Je nach vordefinierten Grenzwerten und Bedingungen wird die Domain in die einschlägigen Datensätze aufgenommen. Dies ist ein kontinuierlicher Prozess. Die Domains werden immer wieder neu bewertet, sobald relevanter Verkehr beobachtet wird.

01

02

03

04

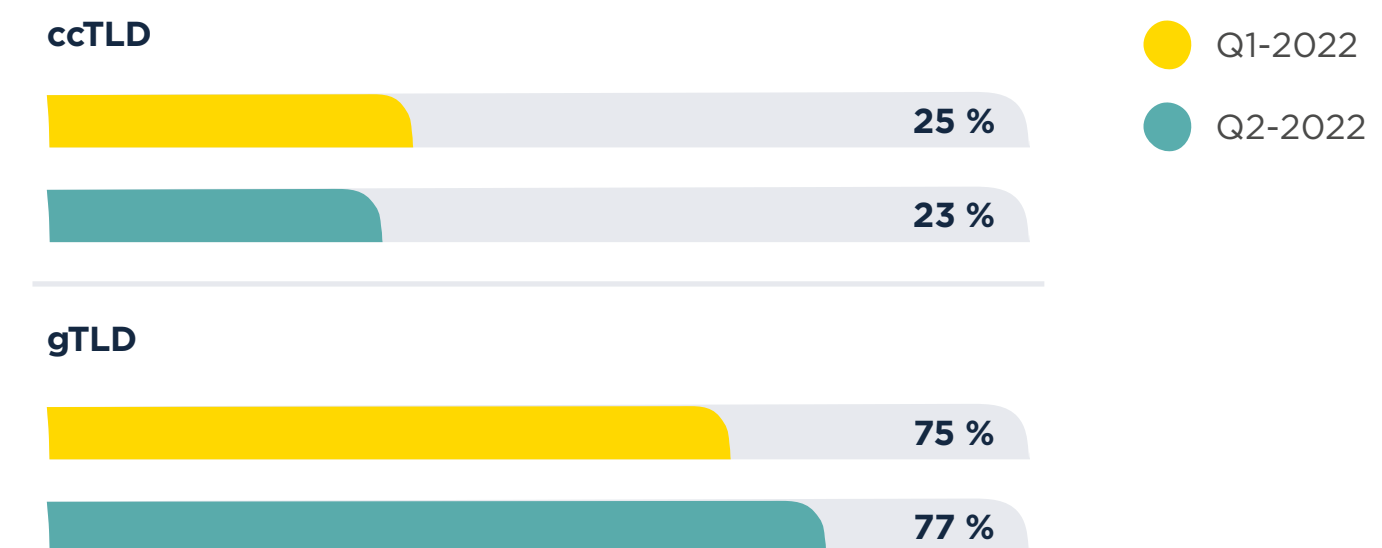
05

In unseren Domain-Daten gelistete TLDs

Die prozentuale Aufteilung zwischen ccTLD und gTLD hat sich im Vergleich zum vorigen Quartal kaum geändert. ccTLDs machen nach wie vor rund ein Viertel der Einträge aus, gTLD drei Viertel.

- **.com** führt die Liste weiterhin an. Viele Angreifer wissen, dass es Szenarien gibt, in denen sich die Verwendung billiger, neuer gTLD-Namen eher negativ auf ihre Aktivitäten auswirkt. Schließlich ist .com der Ort, an dem das Internet stattfindet. Eine .com-Domain erscheint vielen Menschen (und automatisierten Systemen) weniger verdächtig. Berücksichtigt man außerdem die offene Art dieser TLD (jeder kann von überall her eine .com kaufen), ist die Spitzenposition nicht ganz unerwartet.
- **.cn** führt die Liste der ccTLDs an. Wir sehen nach wie vor ein hohes Aufkommen an Phishing-Domains in .cn mit teils lange anhaltender Aktivität. Zweifellos wird die Angelegenheit auch durch die Sprachbarriere erschwert. Für Ausländer ist es schwierig, chinesischen Stellen Probleme zu melden. Umgekehrt ist es für diese Stellen schwierig, die Meldungen zu verstehen und die Fälle zu bewerten.
- **Die Freenom TLDs** erleben weiter missbräuchlich genutzte Registrierungen und „Wegwerf“-Registrierungen in großer Zahl. Selbst mit Antimissbrauchs-APIs halten sich diese TLDs dank des geringen Preises (kostenlos) und der einfachen Registrierung hartnäckig in den Top 20.

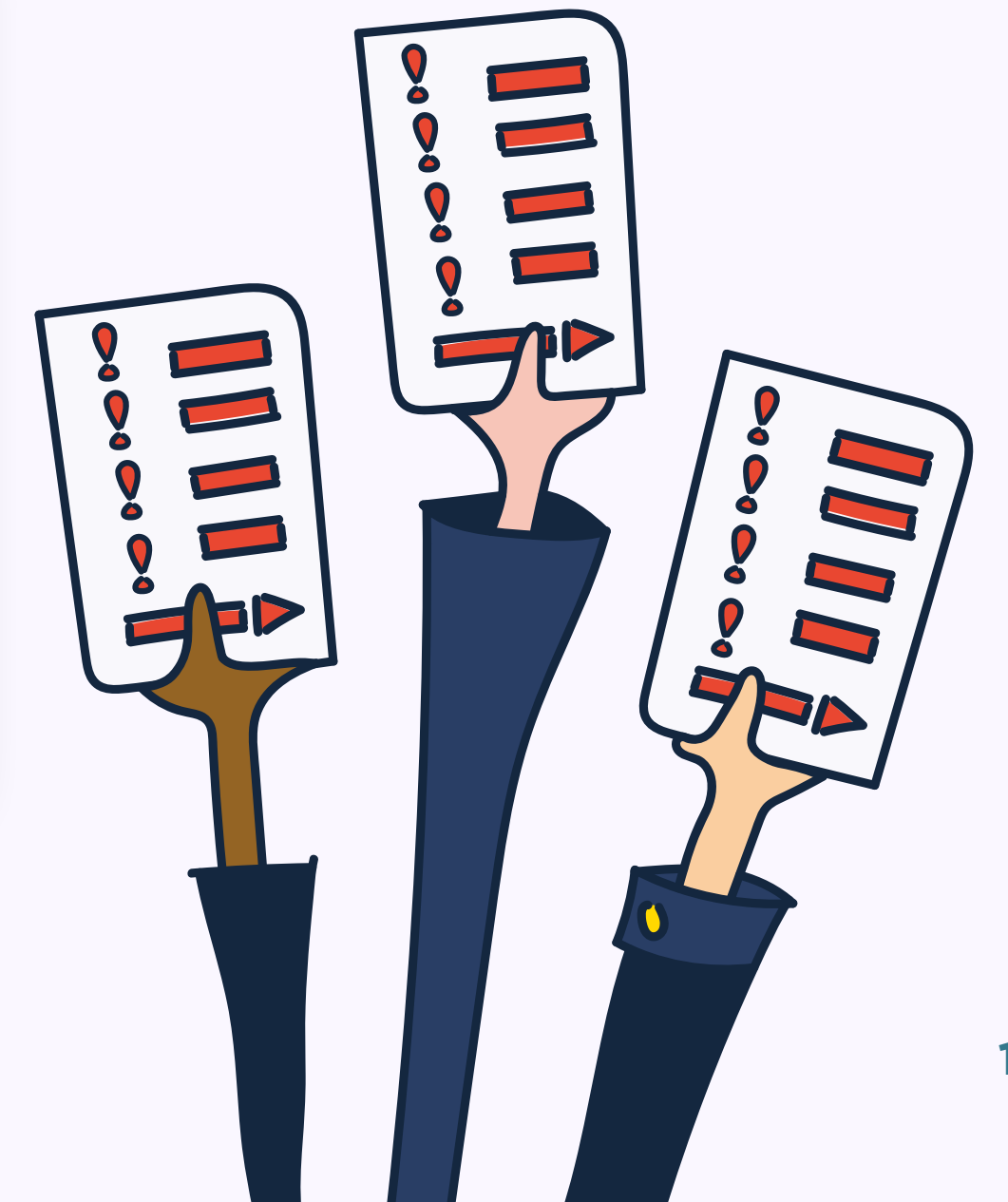
Vergleich der Domain-Einträge nach TLD-Typ gegenüber dem vorigen Quartal



i Auslegung der Daten x

Registrierungsstellen mit einer höheren Anzahl aktiver Domains sind per se anfälliger für Missbrauch. Beispielsweise hatte .net im 2. Quartal 2022 über 13,5 Millionen Domains in seiner Zone, von denen 0,39 % gelistet waren.

.cam hatte gut 36.000 Domains in seiner Zone, von denen 17,03 % in unserem Domain-Datensatz gelistet waren. Beide erscheinen in den Top 20 unserer Listen. Allerdings ist der prozentuale Anteil der gelisteten aktiven Domains bei einem deutlich höher als beim anderen.



01

02

03

04

05



Die Top 20 TLDs ...



Einträge nach ...



Die Top 20 gelisteten TLDs

Rang	Domain TLD	Art der TLD	Q2-2022	Q2-Daten	Q1-2022	% Veränderung
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		-	Neuzugang
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		-	Neuzugang
20	.in	ccTLD	10.346		-	Neuzugang



Die Top 20 TLDs ...



Einträge nach ...



Einträge nach Top 20 ccTLDs

Rang	Domain TLD	Q2-2022	Q2-Daten	Q1-2022	% Veränderung
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		-	Neuzugang
19	.ir	1.615		-	Neuzugang
20	.br	1.479		-	Neuzugang

01

02

03

04

05

Die in Domain-Einträgen verwendeten Top 20 gTLDs

Rang	Domain TLD	Q2-2022	Q2-Daten	Q1-2022	% Veränderung
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		-	Neuzugang
16	.icu	5.929		26.698	▼ -78 %
17	.click	4.339		-	Neuzugang
18	.store	4.118		5.224	▼ -21%
19	.buzz	3.874		16.764	▼ -77%
20	.tokyo	3.484		-	Neuzugang

Top 20 gTLD nach % der Zonendatei mit Domain-Einträgen

Rang	Domain TLD	Q2-2022	Zonengröße	% der Zone sind gelistet	% der Zonendaten
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 %	

01

02

03

04

05



Trendbegriffe ...



Trendbegriffe bei den für Phishing genutzten Domain Names

An der Spitze der Liste steht (wieder einmal) „amazon“ als am häufigsten genutzter Begriff und Markenname bei Phishing-Domains. Gleichzeitig stieg die Beliebtheit von „apple“ bei Phishing-Kampagnen um 104 % und wurde lediglich von „icloud“ mit einem Anstieg um 133 % übertroffen. Ein Begriff verschwand im 2. Quartal jedoch aus den Top 20 der missbrauchten Marken, nämlich „fedex“.

Bei den Phishing-Domains beobachten die Experten von Spamhaus regelmäßig, dass Angreifer im Domain Name eine Handlungsaufforderung verwenden. Die Top 20 spiegeln diesen Trend mit Begriffen wie „verify“, „review“ und „update“. In diesem Quartal stieg „bank“ direkt auf Rang 4 ein, „info“ nur knapp abgeschlagen auf Rang 7.

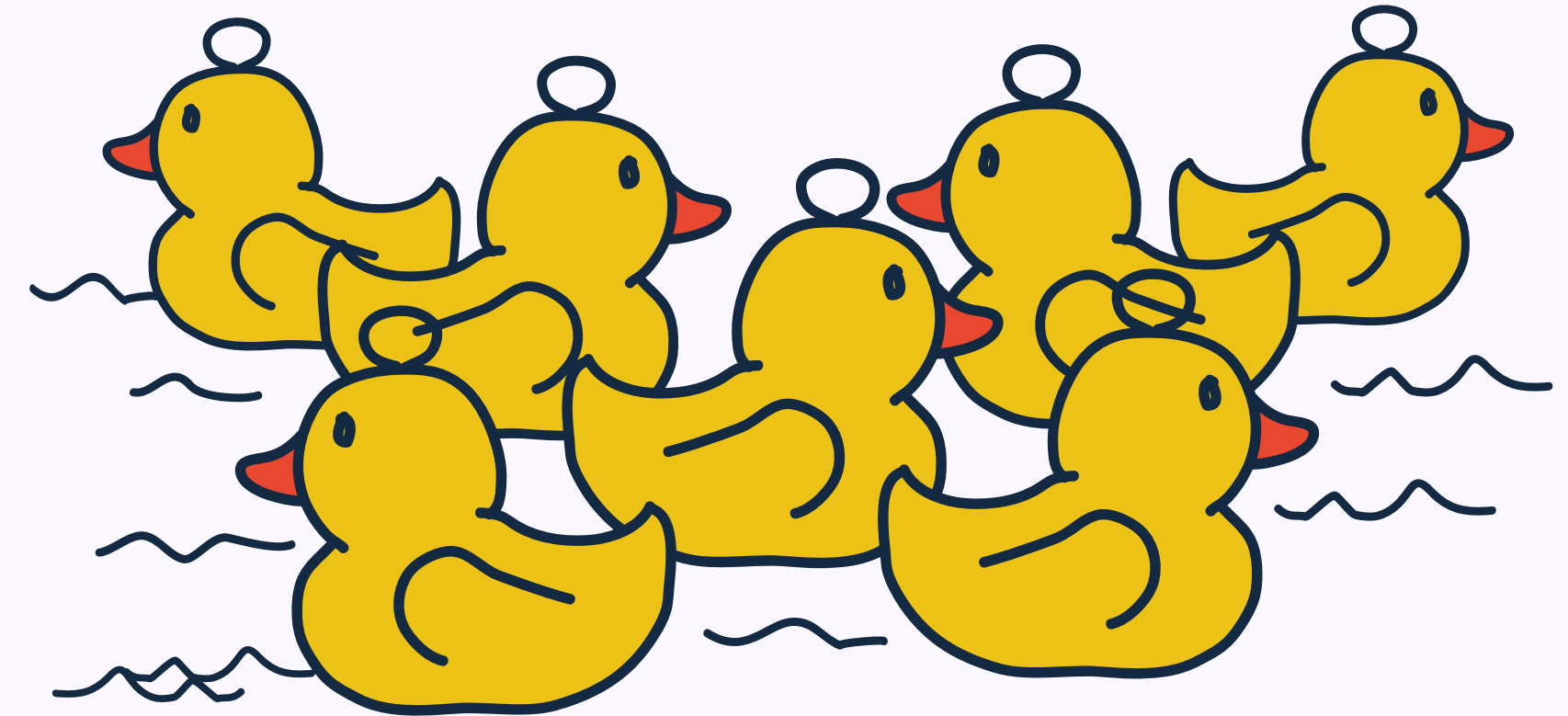


Welche Begriffe nutzen Angreifer für Domain Names?



Einigen Angreifern ist es egal, wie ein Domain Name aussieht, anderen nicht. Die Letzteren bevorzugen eine von zwei Möglichkeiten:

1. Sie versuchen, wie eine legitime Marke zu wirken, indem sie bekannte Markennamen wie z. B. „amazon“ aufnehmen.
2. Sie verwenden Begriffe im Domain Name, die wie eine Aufforderung zum Handeln wirken, z. B. „update now“ und „verify your account“.



05



01

02

03

04

05



Arten von Einträgen

Arten von Einträgen

Im 2. Quartal war Phishing offensichtlich die bevorzugte Art des Missbrauchs beeinträchtigter Domains. Der Anstieg betrug 81 %, während der Missbrauch durch Botnet C&C um 60 % zurückging.

Bei beeinträchtigten Domains, die bösartiges Verhalten aufweisen, sollten Sie Folgendes beachten:

- Die meisten Übergriffe erfolgen automatisch, und Maschinen machen sich keine Gedanken über die zugehörige TLD.
- Viele manipulierte Websites erhalten als zweifelhaftes „Geschenk“ ein Traffic Distribution System (TDS). Damit können Angreifer Inhalte, URLs, und [Geoblocking](#) rotieren. Unsere Experten konnten bei manchen Websites Hunderte einzelner URLs beobachten, einige davon waren schon monatelang aktiv.
- Zurzeit erfolgt ein Großteil der Beeinträchtigungen offensichtlich auf Website-Ebene. Meist enthält

hier ein Content-Management-System (CMS) wie WordPress oder Drupal eine Schwachstelle, über die bösartige Dateien oder Code auf die Website transportiert werden. Angreifer nutzen diese, um „freie“ Domains mit (fast immer) guter Reputation zu erhalten – das Gegenteil zum Kauf einer nagelneuen Domain ohne Reputation. Da die Besitzer legitim sind, profitieren die Angreifer außerdem davon, dass diese Domains nicht abgeschaltet werden.

- In einigen Fällen beobachten wir zudem Beeinträchtigungen auf DNS-Ebene. Diese erfolgen häufig über gestohlene Anmeldedaten von Registrierungsstellen oder über gestohlene oder gehackte Administrationstools wie cPanel oder Plesk. Haben die Angreifer erst einmal die Kontrolle über die autoritative DNS, können sie ganz einfach Hostnamen hinzufügen, die auf ihre eigene Infrastruktur verweisen. Auch hier profitieren sie davon, bestehende Domains mit guter Reputation zu bösartigen Zwecken ausnutzen zu können.



Unterschiede zwischen beeinträchtigten und bösartigen Domains

Bei einer **beeinträchtigten Domain** ist es offensichtlich, dass sie einen legitimen Besitzer hat; allerdings wird sie von einem Angreifer missbraucht. Wird zum Beispiel ein Content-Management-System (CMS) gehackt und wird über die Domain dann Spam versendet, landet die Domain auf unserer Liste. Bei Spamhaus bezeichnen wir diese Art von Einträgen als „abused-legit“.

Eine **bösartige Domain** wird hingegen von der Person registriert, die den Missbrauch begehen will.

Arten von Einträgen

Schlechte Reputation

Bösartig	Beeinträchtigt
969.475	12.715
▼ -16 % ▼	▼ -22 % ▼

Die Punktzahl der Domain-Reputation überschreitet die Grenzwerte der Richtlinie.

Botnet C&C

Bösartig	Beeinträchtigt
4.773	57
▼ -25 % ▼	▼ -60 % ▼

Die Domain wird zur Verwendung durch einen Botnet-Command-and-Controller (C&C) registriert.
(Unterkategorie von „schlechte Reputation“)

Malware

Bösartig	Beeinträchtigt
6.278	4.400
▲ 55 % ▲	▼ -6 % ▼

Die Domain wird für die Verbreitung von Malware genutzt.
(Unterkategorie von „schlechte Reputation“)

Phishing

Bösartig	Beeinträchtigt
278.341	14.630
▲ 6 % ▲	▲ 81 % ▲

Die Domain wird mit Phishing in Zusammenhang gebracht.
(Unterkategorie von „schlechte Reputation“)

01

02

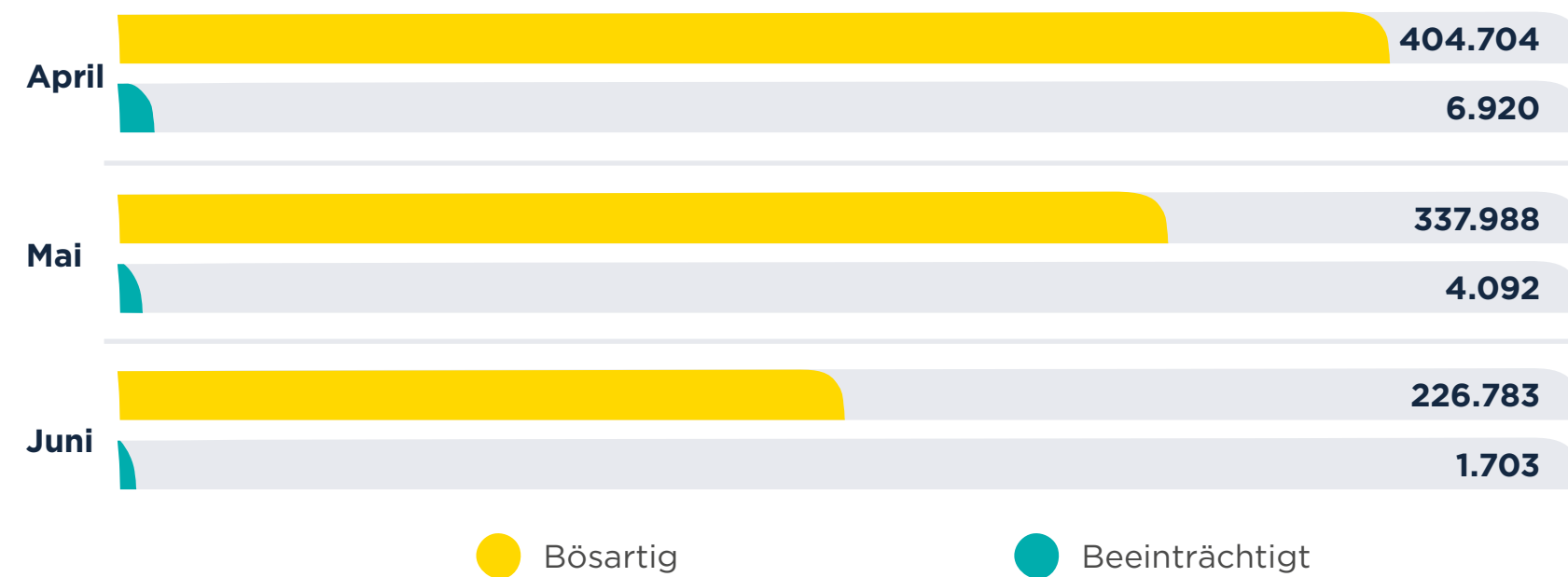
03

04

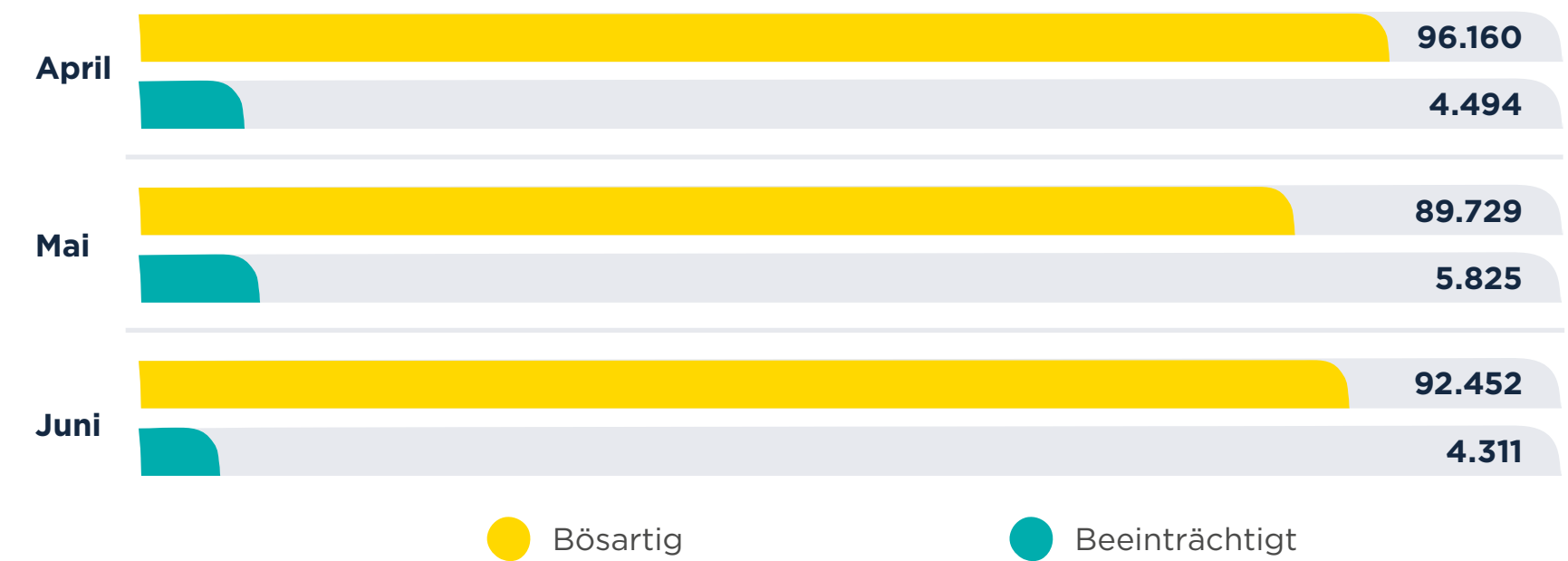
05

Arten von Missbrauch

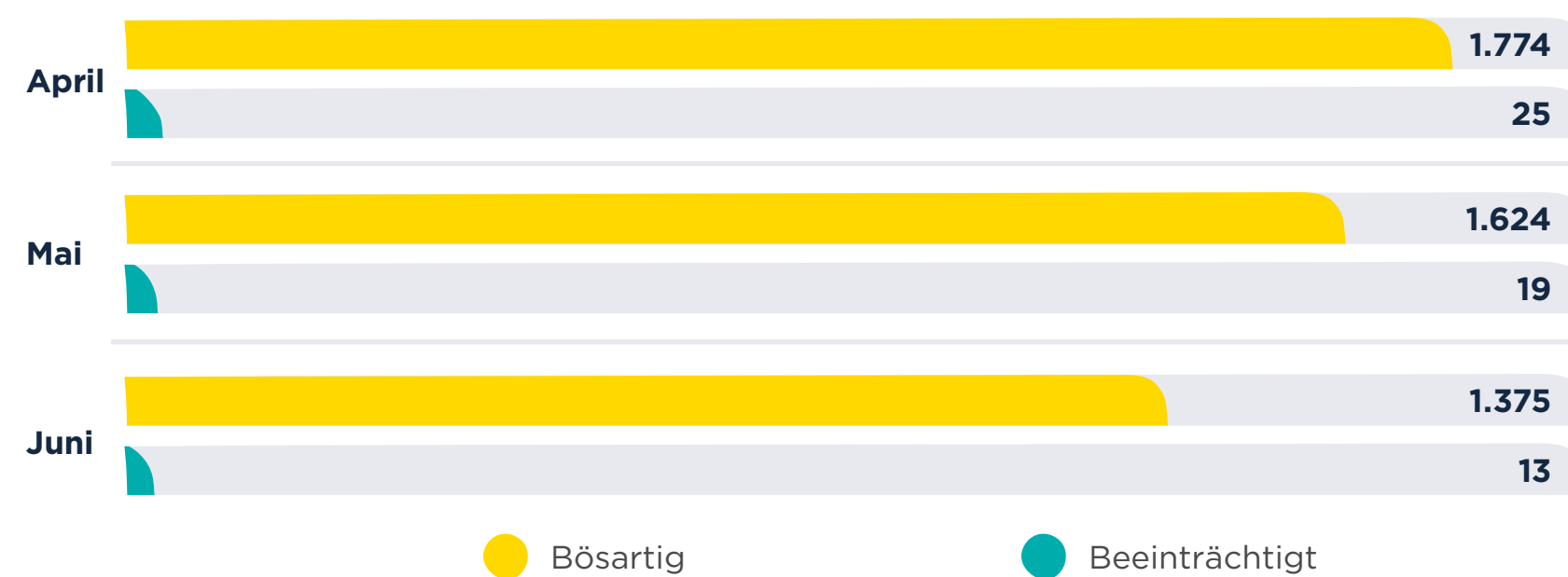
Schlechte Reputation pro Monat



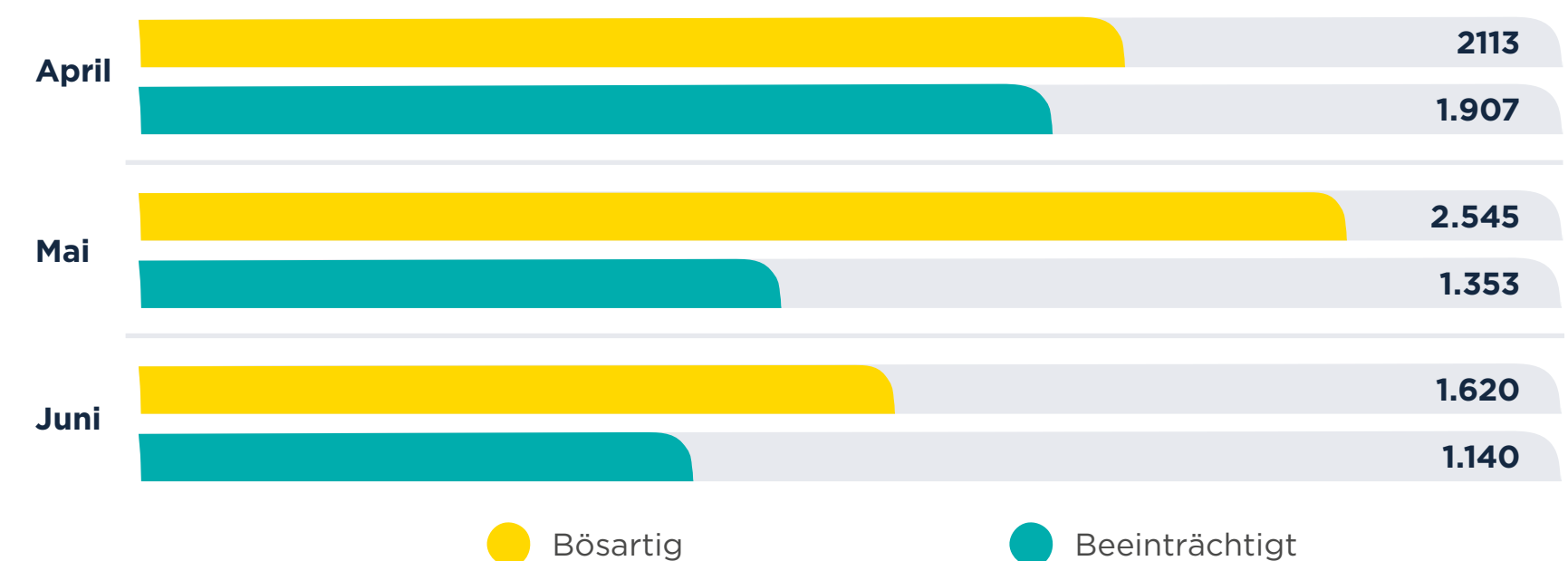
Phishing pro Monat



Botnet C&C pro Monat



Malware pro Monat



01

02

03

04

05

Unsere Quartals-empfehlungen

Da dies der erste veröffentlichte Bericht ist, sprechen wir zunächst einige allgemeine Empfehlungen zur Domain-Name-Reputation für Domain-Besitzer aus. Nicht alle gelten für jeden, und einige erscheinen Ihnen vielleicht sehr allgemein. Trotzdem schadet es nicht, sich diese Dinge bei Entscheidungen bezüglich Ihrer Domain Names in Erinnerung zu rufen.



- **Wenn Sie Ihren Domain Name kontrollieren, achten Sie darauf, dass das so bleibt.** Nutzen Sie für das Domain-Name-Management eine starke, eindeutige Kombination aus Anmelde-ID und Passwort und schützen Sie das Ganze durch 2-Faktor-Authentifizierung.
- **Befindet sich der Host Ihres Domain Name in einem zweifelhaften Netzwerk, ist dies schlecht für die Reputation.** Wie die Art eines Unternehmens eine Nachbarschaft beeinflusst, so kommt auch die Art der Nachbarschaft auf ein Unternehmen zurück. Das gilt auch für Domains!
- **Anonymität trägt nicht zur guten Reputation bei.** Wenn ein Unternehmen einen Domain Name besitzt, muss dieser im WHOIS/RDAP sichtbar sein. Auch wenn der Name eines Unternehmens nicht persönlich identifizierbar ist, wird er von vielen Registrierungsstellen gefiltert.
- **Weniger ist mehr, wenn es um die Anzahl der genutzten Domain Names geht.** Fragen Sie sich beim Kauf zusätzlicher Domain Names, ob Sie nicht besser eine Subdomain Ihrer primären Domain nutzen sollten. Häufig lautet die Antwort „ja“. Sind wirklich zusätzliche Domain Names nötig, müssen diese eng mit dem primären Domain Name verknüpft sein. Berücksichtigen Sie auch, wie sich ein neuer Domain Name beispielsweise auf E-Mail, SEO und die Erwartungen Ihrer Kunden/Zielgruppen auswirkt. Eine neue Domain, die Ihrer bestehenden Domain zu stark ähnelt, wird vielleicht als Phishing gemeldet!

01

02

03

04

05

Weitere Informationen

Über Spamhaus ✕

Spamhaus ist die bewährte Adresse für IP- und Domain-Reputation und genießt aufgrund seiner hohen Ethik, Objektivität und Qualität seiner Daten höchstes Vertrauen in der Branche. Unsere Daten schützen nicht nur, sie bieten auch Analysedaten über Netzwerke und E-Mail-Systeme weltweit.

Seit über 20 Jahren decken unsere Recherspezialisten und Threat Hunter bössartige Aktivitäten auf und machen das Internet zu einem besseren Ort – für alle. Die Daten von Spamhaus werden von Organisationen vieler Branchen genutzt, darunter auch globale Technologieunternehmen. Derzeit schützen die Daten mehr als drei Milliarden Postfächer.

Berichtsmethode ✕

- Spamhaus bezieht seine Daten aus unterschiedlichen Quellen, darunter ISPs und ESPs sowie Unternehmens- und Rechcrhespezialisten. Unser Rechcrheteam analysiert diese Daten mithilfe von maschinellern Lernen, Heuristik und manueller Ermittlung zur Erkennung von bössartigem Verhalten und schlechter Reputation. Die Daten in diesem Bericht entsprechen den bössartigen Domains, die Spamhaus beobachtet, identifiziert und gelistet hat. Sie bilden nicht die Gesamtheit aller bössartigen Domains und aller Domains mit schlechter Reputation im Internet ab.
- Bössartige Kampagnen richten sich regelmäßig gegen bestimmte geografische Gebiete, ISPs oder Organisationen. Auch dieser Faktor kann das Gesamtbild verzerren.
- Aufgrund bestimmter Entwicklungen im Zusammenhang mit WHOIS- und RDAP-Daten, die sich unserer Kontrolle entziehen, sind einige Daten unvollständig. Dies ist eine direkte Folge der Datenschutz-Grundverordnung.
- Wo uns Daten zu Zonendateien fehlen, würden wir es begrüßen, wenn Registrierungsstellen uns diese freundlicherweise zur Verfügung stellen könnten.

01

02

03

04

05