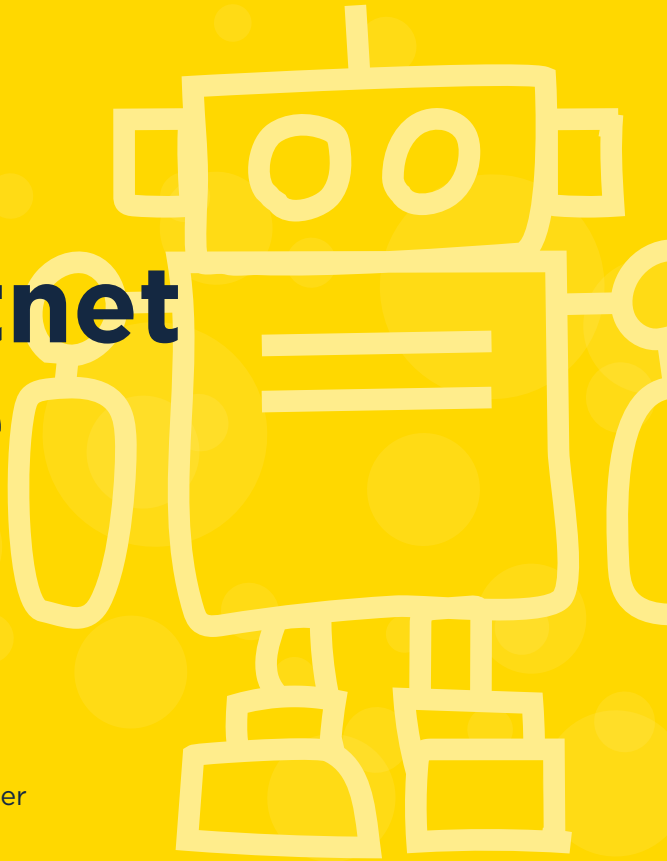
SPAMHAUS

Spamhaus Botnet Threat Update



Q1-2022

Im 1. Quartal 2022 stieg die Zahl der neuen von unserem Rechercheteam identifizierten Botnet-Command-and-Control-Aktivitäten (C&Cs) geringfügig um 8 %. Positiven Entwicklungen wie dem Ende von TrickBot stand unter anderem das fortgesetzte Unvermögen lateinamerikanischer Netzwerkbetreiber entgegen, effektiv mit aktiven Missbrauchsmeldungen umzugehen. Gleichzeitig kam es an Orten, an denen Register und Registrierungsstellen kostenlose bzw. billige Geschäftsmodelle anbieten, zu einem unverhältnismäßigen Anstieg der Missbrauchsfälle.

Willkommen beim Spamhaus Botnet Threat Update für das 1. Quartal 2022.

Über diesen Bericht

Spamhaus verfolgt sowohl IP-Adressen als auch Domain Names, die von Cyberkriminellen als Hosts für Botnet Command-and-Control-Server (C&C-Server) missbraucht werden. Anhand dieser Daten können wir weitere Elemente identifizieren, beispielsweise den geografischen Standort der Botnet C&Cs, die damit verbundene Malware, die bei der Registrierung von Botnet C&Cs verwendeten Top Level Domains einschließlich der Registrierungsstellen sowie das Netzwerk, in dem die Infrastruktur der Botnet C&Cs gehostet wird.

Dieser Bericht bietet einen Überblick über die Zahl der mit diesen Elementen zusammenhängenden Botnet C&Cs im vierteljährlichen Vergleich. Wir erklären die beobachteten Trends und beleuchten, welche Dienstanbieter offensichtlich Probleme damit haben, die Zahl der Botnet-Betreiber einzudämmen, die ihre Dienste missbrauchen.

Im Blickpunkt

Freenom – wenn kostenlose Domains zum Problem werden

Etwas umsonst

Wir freuen uns doch alle, wenn wir für einen Service, den wir nutzen, nichts bezahlen müssen. Freenom, ein in den Niederlanden ansässiger Domain-Registrierungsdienst bietet genau das: kostenlose Domain-Registrierungen für manche Angebote. Gemäß der Website von Freenom[1] ist „Freenom der erste und einzige Anbieter kostenloser Domains“.

Klingt doch super, oder? Von unserer Warte aus betrachtet ist die Antwort ein nachdrückliches „Nein“, denn leider sind kostenlose Dienste erfahrungsgemäß nicht nur für legitime Nutzer und Unternehmen interessant. Vielmehr ziehen sie in der Regel weniger wünschenswerte Nutzer an, die wiederum jede Menge Missbrauch mit sich bringen.

Die problematischen Top Level Domains

Freenom betreibt (über Verträge mit den einschlägigen Registrierungsstellen[2]) die folgenden fünf Country-Code Top Level Domains (ccTLDS):

- .tk (ccTLD von Tokelau)
- .ml (ccTLD von Mali)
- .ga (ccTLD von Gabun)
- .cf (ccTLD der Zentralafrikanischen Republik)
- .gq (ccTLD von Äquatorialguinea)

1 www.freenom.com/en/freeandpaiddomains.html
2 domainincite.com/17468-freenom-ads-gq-to-free-african-cctld-roster

Während Domain-Anmelder in der Regel die ccTLDs ihres jeweiligen Land nutzen, haben sich diese fünf von Freenom für alle möglichen Zwecke betriebenen ccTLDs zu allgemeinen Top Level Domains (gTLDs) entwickelt, die primär außerhalb ihres eigenen Landes genutzt werden.

Und was hat das jetzt mit Missbrauch zu tun?

Wie Sie bei der Lektüre unseres Berichts erkennen werden, erscheinen alle fünf TLDs von Freenom in unseren Vierteljahres-Charts der bei Domain-Registrierungen am häufigsten für Botnet C&Cs missbrauchten TLDs.

Ein genauerer Blick auf unsere Daten zeigt, dass die meisten betrügerischen Domain-Registrierungen bei den TLDs von Freenom nicht von besonders ausgebufften „professionellen" Betrügern vorgenommen werden, sondern von Nutzern frei verfügbarer Crimeware-Kits, die für kleines Geld im Darknet zu beziehen sind. Diese eher „amateurhaften" Betrüger verfügen nicht über die gleichen finanziellen Mittel wie „professionell" agierende Cyberkriminelle. Kein Wunder, dass sie eher versuchen, kostenlose Dienste auszunutzen, wie sie von Freenom angeboten werden.

Nicht nur Botnet C&Cs

Im vergangenen Jahr veröffentlichte PhishLabs einen Bericht über Phishing-Website-TLDs und den Missbrauch von Zertifikaten[1]. Dem Bericht war zu entnehmen, dass sieben der zehn am häufigsten missbrauchten TLDs tatsächlich ccTLDs waren, fünf davon (Sie haben es vermutlich schon erraten) die oben genannten ccTLDs, für die sich Nutzer bei Freenom kostenlos registrieren können.

[1] www.phishlabs.com/blog/breaking-down-phishing-site-tlds-and-certificate-abuse-in-q1/

Wenn Sie sich die Rangliste der zehn am häufigsten missbrauchten TLDs[1] ansehen, welche die „Bösartigkeit“ einer TLD bewertet, werden Sie feststellen, dass alle fünf TLDs von Freenom darin erscheinen.

Die zehn am häufigsten missbrauchten Top Level Domains

Die TLDs mit dem schlechtesten Ruf in puncto Spam (Stand: 14. April 2022):

Rang	Domain	Badness Index	Erkannte Domains	Bösartige Domains	%
1.	**.cn**	3,82	135.203	47.939	35,5 %
2.	**.surf**	3,60	3.182	1.557	48,9 %
3.	**.gq**	2,94	8.976	3.259	36,3 %
4.	**.ga**	2,87	13.717	4.661	34,0 %
5.	**.cf**	2,72	12.431	4.071	32,7 %
6.	**.tk**	2,38	36.192	9.411	26,0 %
7.	**.ml**	2,32	21.396	5.732	26,8 %
8.	**.work**	2,01	34.974	7.830	22,4 %
9.	**.top**	1,79	75.593	14.177	18,8 %
10.	**.cam**	1,56	7.782	1.642	21,1 %

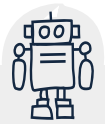
Es ist nicht von der Hand zu weisen: Wo es etwas umsonst gibt, lassen Betrüger nicht lange auf sich warten!

[1] www.spamhaus.org/statistics/tlds/

Anzahl der erkannten Botnet C&Cs, Q1-2022

Im 1. Quartal 2022 identifizierte Spamhaus 3.538 Botnet C&Cs gegenüber 3.271 im 4. Quartal 2021. Das bedeutet einen Anstieg um sage und schreibe 8 % innerhalb eines Quartals. Der Monatsdurchschnitt stieg von 1.090 im 4. Quartal 2021 auf 1.179 Botnet C&Cs im 1. Quartal 2022.

Quartal	Anzahl von Botnets	Quartalsdurchschnitt	% Veränderung
Q2-2021	1462	487	-12 %
Q3-2021	2656	885	+82 %
Q4-2021	3271	1090	+23 %
Q1-2022	3538	1179	+8 %



Was sind Botnet Command-and-Controllers?

Ein „Botnet Controller“, „Botnet C2“ oder „Botnet Command & Control“-Server wird üblicherweise kurz als „Botnet C&C“ bezeichnet. Betrüger nutzen solche Botnet C&Cs, um mit Malware infizierte Rechner zu kontrollieren sowie personenbezogene und andere wertvolle Daten abzugreifen.

Botnet C&Cs spielen eine wichtige Rolle bei Aktivitäten von Cyberkriminellen, die infizierte Rechner dazu missbrauchen, Spam oder Ransomware zu versenden, DDoS-Angriffe zu starten, E-Banking- oder Klickbetrug zu begehen oder Kryptowährungen wie Bitcoin abzuschöpfen.

Desktop-Computer und Mobilgeräte wie Smartphones sind nicht die einzigen Geräte, die infiziert werden können. Immer mehr Geräte sind mit dem Internet verbunden, beispielsweise Geräte im Internet der Dinge (IoT) wie Webcams, Network Attached Storage (NAS) und vieles mehr. Auch diese Geräte laufen Gefahr, infiziert zu werden.

Geografische Verteilung der Botnet C&C Hosts, Q1-2022

Ein Jahr des Anstiegs für Russland

Im vergangenen Jahr legte die Anzahl der Botnet C&Cs in Russland von Quartal zu Quartal zu:

- Q1 bis Q2-2021 – Zunahme um 19 %
- Q2 bis Q3-2021 – Zunahme um 64 %
- Q3 bis Q4-2021 – Zunahme um 124 %
- Q4-2021 bis Q1-2022 – Zunahme um 24 %

Im 1. Quartal befand sich rund ein Drittel aller von unseren Recherche-Experten aufgedeckten Botnet C&C Server in Russland.

Zunahme der im Westen gehosteten Botnet C&Cs

Neben dem kontinuierlichen Anstieg der in Russland gehosteten Botnet C&Cs beobachten wir auch im Westen eine Zunahme, insbesondere in der Ukraine (+80 %), Frankreich (+23 %), den USA (+20 %), den Niederlanden (+16 %) und Estland (Neueinstieg). Der Anstieg in der Ukraine ist angesichts des dort herrschenden Krieges nicht überraschend – Betrüger zählen zu den Ersten, die Schwachstellen erkennen und ausnutzen.

Marginale Verbesserungen in Lateinamerika

Ende 2021 verzeichneten die lateinamerikanischen Länder einen deutlichen Anstieg der dort gehosteten Botnet C&Cs. In diesem Quartal war ein leichter Rückgang dieser Zahlen zu beobachten: Uruguay (–4 %), Mexiko (–12 %), Brasilien (–20 %), mit Ausnahme der Dominikanischen Republik, in der ein Anstieg von 16 % zu verzeichnen war. Im Umgang mit Missbrauch gibt es in dieser Region noch viel Luft nach oben.

Neuzugänge

Vereinigte Arabische Emirate (15), Estland (16).

Abgänge

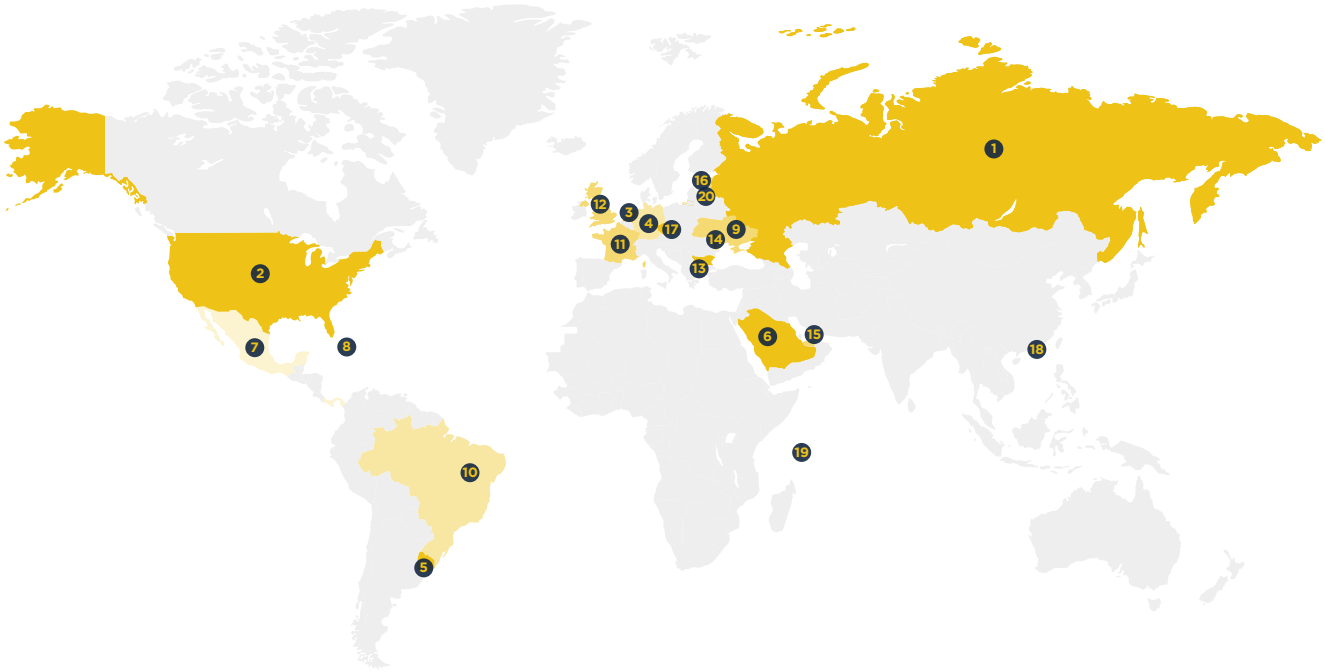
Schweden, Rumänien.

Geografische Verteilung der Botnet C&Cs, Q1-2022 (Fortsetzung)

Top 20 Botnet C&C-Hosting-Länder

Rang	Land	Q4-2021	Q1-2022	% Veränderung zum Vorquartal
1.	Russland	854	1059	24 %
2.	USA	384	461	20 %
3.	Niederlande	164	191	16 %
3.	Deutschland	230	191	-17 %
5.	Uruguay	177	170	-4 %
6.	Saudi-Arabien	180	163	-9 %
6.	Mexiko	186	163	-12 %
8.	Dominikanische Republik	110	128	16 %
9.	Ukraine	64	115	80 %
10.	Frankreich	60	74	23 %

Rang	Land	Q4-2021	Q1-2022	% Veränderung zum Vorquartal
10.	Brasilien	92	74	-20 %
12.	Großbritannien	61	64	5 %
13.	Bulgarien	56	62	11 %
14.	Moldawien	50	54	8 %
15.	VAE	-	47	Neuzugang
16.	Estland	-	45	Neuzugang
17.	Tschechische Republik	66	40	-39 %
18.	Hongkong	28	38	36 %
19.	Seychellen	34	37	9 %
19.	Lettland	69	37	-46 %



Mit Botnet C&Cs assoziierte Malware, Q1-2022

Achtung, Spoiler! An der Spitze der vierteljährlichen Malware-Charts gab es keine Veränderung – RedLine und Loki, beides Credential Stealer, führen unsere Liste weiterhin an.

Malware-as-a-Service

Zwar ist die Anzahl der RedLine Botnet C&C Server leicht zurückgegangen, dafür haben die Loki-Server um 47 % zugelegt. Beide werden im Darknet als „Crimeware Kit" verkauft, mit dem jeder Käufer seine eigene Malware betreiben kann.

Auf Nimmerwiedersehen, TrickBot!

Viele Jahre lang war TrickBot einer der größten Botnets, der es immer wieder in unsere Top 20 schaffte. Ursprünglich ein E-Banking-Trojaner, entwickelte sich TrickBot im Laufe der Zeit zum Dropper und verschaffte Cyberkriminellen den Zugriff auf betriebliche Netzwerke. In dieser Funktion wurde TrickBot zum ernsten Problem für die US-Wirtschaft und war für Cyberangriffe gegen hunderte amerikanischer Unternehmen verantwortlich.

2020 überlebte TrickBot Takedown-Versuche sowohl von Microsoft als auch vom US Cyber Command[1]. Im 1. Quartal 2022 verschwand TrickBot urplötzlich von der Malware-Bildfläche. Sicherheitsexperten bestätigten in einem Tweet[2] die Abschaltung sowohl des Betriebs als auch der Infrastruktur des notorischen TrickBot-Malware-Akteurs. Adieu TrickBot – wir werden dich nicht vermissen!

Tofsee, Smoke Loader und Arkei gewinnen weiterhin an Beliebtheit

2021 stiegen die drei oben Genannten in die Top 20 ein und konnten im vergangenen Vierteljahr Zunahmen von 100 % und mehr verzeichnen!

Was ist ein Credential Stealer?

Cyberkriminelle nutzen Credential Stealer, um sensible Daten wie beispielsweise Anmeldedaten vom Rechner eines Opfers abzugreifen.

Neuzugänge

AveMaria (Rang 14), Quasar (17), CoinMiner (18), DanaBot (20).

Abgänge

CobaltStrike, CryptBot, Gozi, TrickBot.

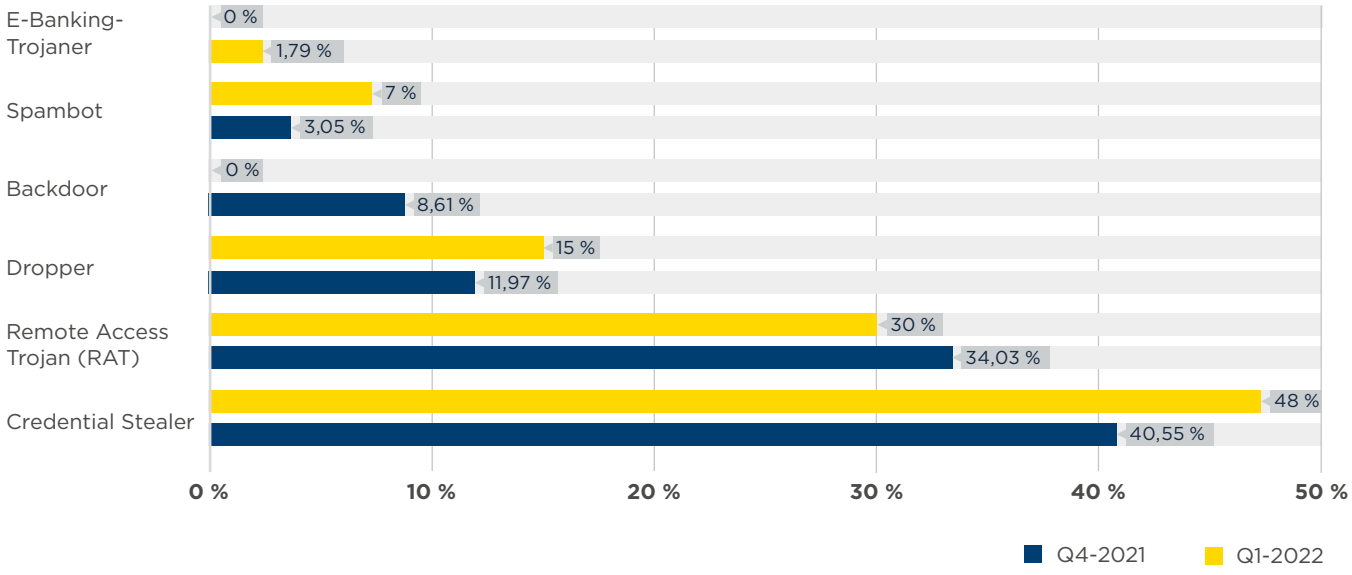
1 www.cyberscoop.com/trickbot-takedown-cyber-command-microsoft/
2 twitter.com/VK_Intel/status/1496944228135493638

Mit Botnet C&Cs assoziierte Malware, Q1-2022 (Fortsetzung)

Mit Botnet C&Cs assoziierte Malware-Familien

Rang	Q4-2021	Q1-2022	% Veränderung	Malware-Familie	Beschreibung
1.	164	153	-7 %	RedLine	Credential Stealer
2.	102	150	47 %	Loki	Credential Stealer
3.	91	74	-19 %	AsyncRAT	Remote Access Trojan (RAT)
4.	86	66	-23 %	GCleaner	Dropper
5.	29	59	103 %	Tofsee	Spambot
5.	28	59	111 %	Smoke Loader	Dropper
7.	27	54	100 %	Arkei	Credential Stealer
8.	75	37	-51 %	Raccoon	Credential Stealer
9.	32	32	0 %	DCRat	Remote Access Trojan (RAT)
10.	17	26	53 %	NanoCore	Remote Access Trojan (RAT)
11.	29	23	-21 %	Remcos	Remote Access Trojan (RAT)
12.	17	22	29 %	STRRAT	Remote Access Trojan (RAT)
13.	36	20	-44 %	NjRAT	Remote Access Trojan (RAT)
14.	-	19	Neuzugang	AveMaria	Remote Access Trojan (RAT)
15.	18	18	0 %	Socelars	Credential Stealer
16.	37	16	-57 %	BitRAT	Remote Access Trojan (RAT)
17.	-	13	Neuzugang	Quasar	Remote Access Trojan (RAT)
18.	65	12	-82 %	Vjw0rm	Remote Access Trojan (RAT)
18.	-	12	Neuzugang	CoinMiner	Cryptocurrency Miner
20.	-	10	Neuzugang	DanaBot	Credential Stealer

Vergleich der Malware-Typen zwischen Q4-2021 und Q1-2022



Die am häufigsten missbrauchten Top Level Domains, Q1-2022

Die am häufigsten missbrauchten Top Level Domains, Q1-2022

Es überrascht nicht, dass es keine Veränderung an der Spitze unseres Quartalsrankings gegeben hat. gTLD.com ist weiterhin die von Malware-Entwicklern und Botnet-Betreibern bei der Registrierung ihrer Domain Names bevorzugte TLD.

Auf Platz 2 liegt weiterhin gTLD.top aus China. Allerdings waren im 1. Quartal auch gewisse Verbesserungen zu verzeichnen, beispielsweise ein Rückgang der neu erkannten Botnet C&C Domains um immerhin 30 %. Allerdings war die Anzahl der mit Botnet C&Cs assoziierten Domains bei .top immer noch mehr als doppelt so hoch wie bei .xyz auf Platz 3.

Neuzugang an Nr. 4

In diesem Quartal stieg .us direkt auf Platz 4 in die Top 20 ein. Bleibt zu hoffen, dass GoDaddy, die für .us verantwortlich sind, dem Beispiel von .buzz folgen, die vor einem Jahr auf Platz 3 in unsere Charts einstiegen, in diesem Quartal jedoch wieder daraus verschwunden sind. Glückwunsch an .buzz für den konsequenten Umgang mit dem der TLD dotStrategy zugeschriebenen Missbrauch – und höchste Zeit für GoDaddy, ebenso zu handeln!

Abgänge

Gratulation an alle Registrierungsstellen mit TLDs, die wieder aus unseren Listen verschwunden sind, einschließlich ICM, die für .xxx verantwortlich sind. Diese TLD stieg im 4. Quartal 2021 auf Platz 4 in unsere Top 20 ein, tritt dort in diesem Quartal jedoch nicht mehr in Erscheinung.

Deutlicher Rückgang bei .com und .net von Verisign

Die TLDs .com und .net (beide Verisign) konnten mit –75 % bzw. –61 % die stärksten Rückgänge im 1. Quartal verzeichnen, dicht gefolgt von .xyz mit –52 %. Gute Leistung, weiter so!

Top Level Domains (TLDs) – eine Übersicht

Es gibt mehrere verschiedene Top Level Domains, darunter:

Generische TLDs (gTLDs)
Diese können von jedem genutzt werden.

Länderspezifische TLDs (ccTLDs)
Bei einigen ist die Nutzung auf ein bestimmtes Land oder eine bestimmte Region beschränkt. Andere sind jedoch für die allgemeine Nutzung lizenziert, was sie auf die gleiche Funktionalitätsstufe wie gTLDs stellt.

Dezentralisierte TLDs (dTLDs)
Dies sind unabhängige Top Level Domains, die nicht der Kontrolle der ICANN unterliegen.

Die am häufigsten missbrauchten Top Level Domains, Q1-2022 (Fortsetzung)

.tk, .cf, .ml, .ga und .gq

Im Blickpunkt dieses Quartals stehen die Probleme mit diesen fünf ccTLDs, die aktuell von Freenom betrieben werden. Sie stellen nach wie vor eine ernste Bedrohung für Internetnutzer und Unternehmen dar. Im 1. Quartal 2022 haben wir insgesamt 579 Botnet C&C-Domains identifiziert, die im Domain-Namensraum von Freenom registriert sind. Ein starkes Stück!

Neuzugänge

.us (Rang 4), .website (13), .cn (18), .live (19), .cfd (20)

Abgänge

.br, .buzz, .one, .site, .xxx

Mehr als doppelt so viele betrügerische Domain-Registrierungen bei .sbs und .cloud

Die Zahl der betrügerischen Domain-Registrierungen, die Spamhaus in den beiden gTLDs .sbs und .cloud erkannt hat, hat sich im 1. Quartal 2022 mit einer Zunahme von 145 % (.sbs) bzw. 140 % (.cloud) mehr als verdoppelt.

Bereits im vergangenen Jahr wiesen wir darauf hin, dass unsere Recherche-Experten verstärkt Aktivitäten im Zusammenhang mit .sbs vermelden[1]. Leider sind unsere Warnungen offensichtlich auf taube Ohren gestoßen. Wir fordern die betroffenen Registrierungsstellen ShortDot und Aruba PEC SpA dringend auf, wirksame Maßnahmen zur Verringerung der Anzahl der in ihrem Domain-Namensraum registrierten Botnet C&C-Domains zu treffen.

Auslegung der Daten

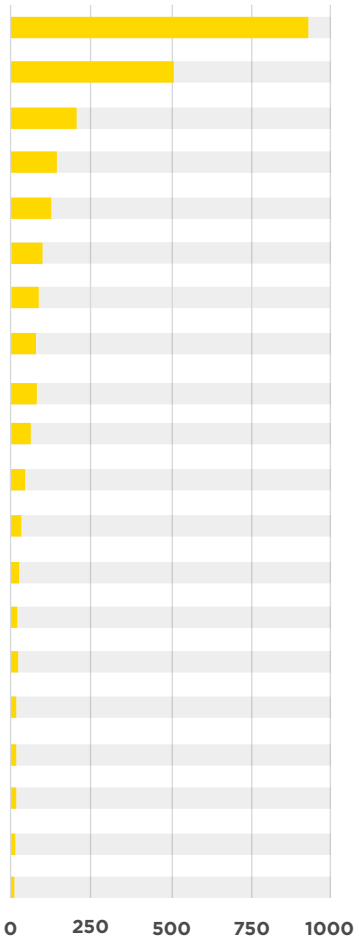
Registrierungsstellen mit einer höheren Anzahl aktiver Domains sind per se anfälliger für Missbrauch. Beispielsweise hatte .net im 1. Quartal 2022 über 6,3 Millionen aktive Domain-Zonen, von denen 0,00093 % mit Botnet C&Cs in Verbindung gebracht wurden. Hingegen hatte .sbs gut 30.000 aktive Domain-Zonen, von denen 0,42 % mit Botnet C&Cs assoziiert wurden. Beide erscheinen in den Top 20 unserer Listen, allerdings ist der prozentuale Anteil aktiver Domains, die mit Botnet C&Cs assoziiert werden, bei einem deutlich höher als beim anderen.

[1] www.spamhaus.com/resource-center/we-hope-you-keep-sbs-clean-shortdot/

Die am häufigsten missbrauchten Top Level Domains, Q1-2022 (Fortsetzung)

Die am häufigsten missbrauchten TLDs – Anzahl der Domains

Rang	Q4-2021	Q1-2022	% Veränderung	TLD	Typ
1.	3719	913	-75 %	com	gTLD
2.	715	501	-30 %	Top	gTLD
3.	396	192	-52 %	xyz	gTLD
4.	-	165	Neuzugang	us	gTLD
5.	122	159	30 %	tk	Ursprünglich ccTLD, jetzt effektiv gTLD
6.	116	137	18 %	org	gTLD
7.	97	126	30 %	cf	Ursprünglich ccTLD, jetzt effektiv gTLD
8.	51	125	145 %	sbs	gTLD
8.	52	125	140 %	cloud	gTLD
10.	87	115	32 %	ml	Ursprünglich ccTLD, jetzt effektiv gTLD
11.	143	106	-26 %	ga	Ursprünglich ccTLD, jetzt effektiv gTLD
12.	56	73	30 %	gq	Ursprünglich ccTLD, jetzt effektiv gTLD
13.	-	70	Neuzugang	website	gTLD
14.	103	67	-35 %	info	gTLD
15.	133	66	-50%	ru	ccTLD
16.	44	59	34 %	de	ccTLD
17.	136	53	-61 %	net	gTLD
18.	-	45	Neuzugang	cn	ccTLD
19.	-	43	Neuzugang	live	gTLD
20.	-	42	Neuzugang	cfd	gTLD



Am häufigsten missbrauchte Domain-Registrierungsstellen, Q1-2022

Keine Veränderung an der Spitze

Leider gibt es keine Veränderung an der Spitze unserer Charts, an der sich NameSilo und Namecheap weiterhin auf Platz 1 bzw. 2 behaupten.

Allerdings haben sich die USA knapp (mit weniger als 1 % Vorsprung) an Kanada vorbeigeschoben und sind jetzt das Land, in dem die meisten missbrauchten Domain-Registrierungsstellen beheimatet sind.

Google neu in den Top 20

Eine herbe Enttäuschung ist Google, die auf Platz 16 erstmalig in unseren Top 20 vertreten sind. Wir hoffen, dass es sich dabei nur um einen einmaligen Ausrutscher handelt und dass Google solide Maßnahmen ergreifen wird, um die Anzahl der Domain-Registrierungen für Botnet C&Cs in seinen Reihen zu verringern.

Wie ist die Lage bei Sav?

Im 1. Quartal erlebte Sav einen Anstieg von 156 %, d. h. von 66 auf 169 registrierte Botnet C&C-Domain-Namen und liegt damit auf Rang 6. Vor Kurzem meldete Sav die Verdopplung der Zahl der vom Unternehmen verwalteten Domains auf zwei Millionen in nur sechs Monaten[1]. Die Anzahl der zwecks Botnet C&C-Missbrauch registrierten Domains hat sich im vergangenen Quartal allerdings mehr als verdoppelt. Muss exponentielles Wachstum zwangsläufig mit exponentiellem Missbrauch einhergehen? Wir glauben nicht.

Verbesserungen bei den Registrierungsstellen

Doch es gibt nicht nur schlechte Nachrichten. Im 1. Quartal haben sich sechs Domain-Registrierungsstellen aus unseren Top 20 verabschiedet, weitere 13 melden Verbesserungen, darunter Key Systems (–91 %), WebNic (–90 %) und Openprovider (–62 %). Glückwunsch an alle Registrierungsstellen, denen der Ausstieg aus unseren Ranglisten gelungen ist, und „weiter so“ an alle, welche die eine Verringerung missbräuchlich registrierter Domains zu verzeichnen haben. Nicht nachlassen!

Registrierungsstellen und Botnet C&C-Betreiber

Cyberkriminelle müssen eine Registrierungsstelle finden, um einen Botnet C&C Domain Name registrieren zu lassen. Registrierungsstellen können unmöglich alle betrügerischen Registrierungen aufdecken, bevor diese Domains online gehen.
Allerdings ist die Lebenserwartung krimineller Domains bei einer legitimen, gut geführten Registrierungsstelle recht kurz.

Neuzugänge

Todaynic (Rang 5), Ligne (13), CentralNic (14), GMO (15), Google (16).

Abgänge

1API, Atak, Beget LLC, Eranet International, Mat Bao Corp, NauNet.

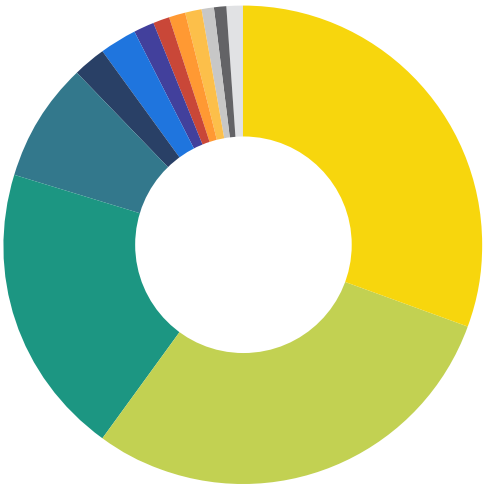
[1] www.dnjournal.com/archive/lowdown/2022/dailyposts/20220409.htm

Am häufigsten missbrauchte Domain-Registrierungsstellen, Q1-2022 (Fortsetzung)

Am häufigsten missbrauchte Domain-Registrierungsstellen – Anzahl der Domains

Rang	Q4-2021	Q1-2022	% Veränderung	Registrierungsstelle	Land
1.	988	847	-14 %	NameSilo	Kanada
2.	718	670	-7 %	Namecheap	USA
3.	536	266	-50%	nicenic.net	China
4.	433	255	-41 %	PDR	Indien
5.	-	236	Neuzugang	Todaynic	China
6.	66	169	156 %	Sav	USA
7.	80	96	20 %	Porkbun	USA
8.	201	88	-56 %	Alibaba	China
9.	127	87	-31 %	Tucows	Kanada
10.	197	75	-62 %	Openprovider	Niederlande
11.	124	73	-41 %	RegRU	Russland
12.	57	50	-12 %	Hostinger	Litauen
13.	-	36	Neuzugang	Ligne	Frankreich
14.	-	35	Neuzugang	CentralNic	Großbritannien
15.	-	31	Neuzugang	GMO	Japan
16.	-	30	Neuzugang	Google	USA
16.	54	30	-44 %	dnspod.cn	China
18.	328	28	-91 %	Key Systems	Deutschland
18.	48	28	-42 %	EuroDNS	Luxemburg
20.	272	27	-90 %	WebNic.cc	Singapur

Standort der am häufigsten missbrauchten Domain-Registrierungsstellen



Land	Q4-2021	Q1-2022
USA	20,43 %	30,57 %
Kanada	26,37 %	29,59 %
China	18,70 %	19,64 %
Indien	10,24 %	8,08 %
Niederlande	4,66 %	2,38 %
Russland	2,93 %	2,31 %
Litauen	1,35 %	1,58 %
Frankreich	0,00 %	1,14 %
Großbritannien	0,00 %	1,11 %
Japan	0,00 %	0,98 %
Deutschland	7,76 %	0,89 %
Luxemburg	1,14 %	0,89 %
Singapur	6,43 %	0,86 %

Netzwerke, welche die meisten neu erkannten Botnet C&Cs hosten, Q1-2022

Wie üblich gab es eine ganze Reihe von Veränderungen bei den Netzwerken, die neu erkannte Botnet C&Cs hosten.

Zeigt diese Liste, wie schnell man in den Netzwerken auf Missbrauch reagiert?

Zwar zeigt diese Top-20-Liste, dass die Überprüfung der Kunden möglicherweise unzureichend ist, sie lässt jedoch keinen Aufschluss darüber zu, wie schnell sich die zuständigen Stellen der gemeldeten Probleme annehmen. Netzwerke, die sich nicht zeitnah um die Behebung von Missbrauchsfällen kümmern, finden Sie unter „Netzwerke, welche die aktivsten Botnet C&Cs hosten“.

Viele Neuzugänge aus Russland

Bei der Durchsicht unserer aktuellen Top 20 fällt eines direkt ins Auge, und das ist die Zahl der Neuzugänge aus Russland.

Im 1. Quartal 2022 handelte es sich bei sechs der acht Neueinsteiger um Hosting-Provider aus Russland. Zusammen hosten sie mehr als 39 % aller Botnet C&Cs – mehr als dreimal so viele wie im 4. Quartal 2021.

Netzwerk- und Botnet C&C-Betreiber

Netzwerke haben ein gewisses Maß an Kontrolle über Betreiber, die sich in betrügerischer Absicht bei einem neuen Dienst anmelden.

Es empfiehlt sich, ein solides Verfahren für die Überprüfung neuer Kunden durchzuführen, anstatt leichtfertig einen Dienst in Betrieb zu nehmen.

Haben Netzwerke viele Listungen, lässt das häufig auf die folgenden Probleme schließen:

1. Die Netzwerke wenden keine praxisbewährten Verfahren zur Kundenüberprüfung an.
2. Die Netzwerke stellen nicht sicher, dass ALLE Reseller solide Kundenüberprüfungsverfahren einhalten.

In den schlimmsten Szenarien profitieren Mitarbeiter oder Inhaber der Netzwerke direkt von betrügerischen Registrierungen, d. h. sie verdienen ihr Geld wissentlich mit Betrügern, die dort ihre Botnet C&Cs hosten. Glücklicherweise sind solche Fälle jedoch selten.

Neuzugänge

vdsina.ru (Rang 7), macloud.ru (9), digitalenergy.online (12), invs.ru (12), ghostnet.de (14), filanco.ru (15), gcore.lu (16), sprinthost.ru (17), hostsailor.com (18).

Abgänge

firstbyte.ru, hetzner.de, itldc.com, m247.ro, nano.lv, pinvds.com, privacyfirst.sh, serverion.com, timeweb.ru

Netzwerke, welche die meisten neu erkannten Botnet C&Cs hosten, Q1-2022 (Fortsetzung)

Neu erkannte Botnet C&Cs pro Netzwerk

Rang	Q4 2021	Q1 2022	% Veränderung	Netzwerk	Land
1.	175	170	-3 %	antel.net.uy	Uruguay
2.	187	163	-13 %	uninet.net.mx	Mexiko
3.	168	153	-9 %	stc.com.sa	Saudi-Arabien
4.	110	128	16 %	claro.com.do	Dominikanische Republik
5.	80	121	51 %	baxet.ru	Russland
6.	182	95	-48 %	alibaba-inc.com	China
7.	-	69	Neuzugang	vdsina.ru	Russland
7.	85	69	-19 %	telefonica.com.br	Brasilien
9.	-	63	Neuzugang	macloud.ru	Russland
9.	48	63	31 %	hostwinds.com	USA
9.	63	63	0 %	selectel.ru	Russland
12.	-	62	Neuzugang	digitalenergy.online	Russland
12.	-	62	Neuzugang	invs.ru	Russland
14.	-	61	Neuzugang	ghostnet.de	Deutschland
15.	-	54	Neuzugang	filanco.ru	Russland
16.	-	53	Neuzugang	gcore.lu	Luxemburg
17.	-	52	Neuzugang	sprinthost.ru	Russland
18.	-	51	Neuzugang	hostsailor.com	VAE
18.	36	51	42 %	ihor-hosting.ru	Russland
20.	72	49	-32 %	cloudflare.com	USA

Netzwerke, welche die aktivsten Botnet C&Cs hosten, Q1-2022

Hosting-Provider, die in dieser Rangliste erscheinen, haben entweder ein Missbrauchsproblem, treffen keine geeigneten Maßnahmen, wenn sie Meldungen über missbräuchliche Nutzungen erhalten oder sie benachrichtigen uns nicht, wenn ein Problem behoben wurde.

Neuzugänge

cableonda.net (Rang 12), eliteteam.to (15), ntup.net (15), alexhost.md (17), selectel.ru (19).

Abgänge

algartelecom.com.br, charter.com, clouvider.net, ovpn.com, une.net.co.

Lateinamerikanische Netzwerkbetreiber weiter mit Missbrauchsproblemen

Wie im jüngsten Botnet Update bereits gemeldet, fällt es Betreibern aus Lateinamerika weiterhin offensichtlich schwer, zeitnah auf Missbrauchsmeldungen zu reagieren. Im 1. Quartal 2022 war diese Region nach wie vor für 60 % der aktiven Botnet C&Cs verantwortlich. Vier der fünf höchstplatzierten Hosting-Unternehmen sind in Lateinamerika ansässig.

Spamhaus fordert diese Betreiber dringend auf, gemeinsam mit Spamhaus gegen den Missbrauch in ihren Netzwerken vorzugehen.

Gesamtzahl aktiver Botnet C&Cs pro Netzwerk

Rang	Q4-2021	Q1-2022	% Veränderung	Netzwerk	Land
1.	389	501	29 %	uninet.net.mx	Mexiko
2.	296	422	43 %	stc.com.sa	Saudi-Arabien
3.	257	398	55 %	antel.net.uy	Uruguay
4.	204	315	54 %	claro.com.do	Dominikanische Republik
5.	146	198	36 %	telefonica.com.br	Brasilien
6.	94	94	0 %	microsoft.com	USA
7.	60	83	38 %	a1.bg	Bulgarien
8.	91	79	-13 %	ipjetable.net	Frankreich
9.	25	65	160 %	ielo.net	Frankreich
10.	41	41	0 %	telefonica.com.ar	Argentinien
11.	27	34	26 %	mobily.com.sa	Saudi-Arabien
12.	29	29	0 %	tie.cl	Chile
12.	-	29	Neuzugang	cableonda.net	Panama
14.	29	28	-3 %	vietserver.vn	Vietnam
15.	-	25	Neuzugang	eliteteam.to	Seychellen
15.	-	25	Neuzugang	ntup.net	Russland
17.	21	24	14 %	google.com	USA
17.	-	24	Neuzugang	alexhost.md	Moldawien
19.	-	23	Neuzugang	selectel.ru	Russland
20.	21	22	5 %	combahton.net	Deutschland

Damit verabschieden wir uns für heute. Im Juli sehen wir uns wieder. Bleiben Sie gesund!