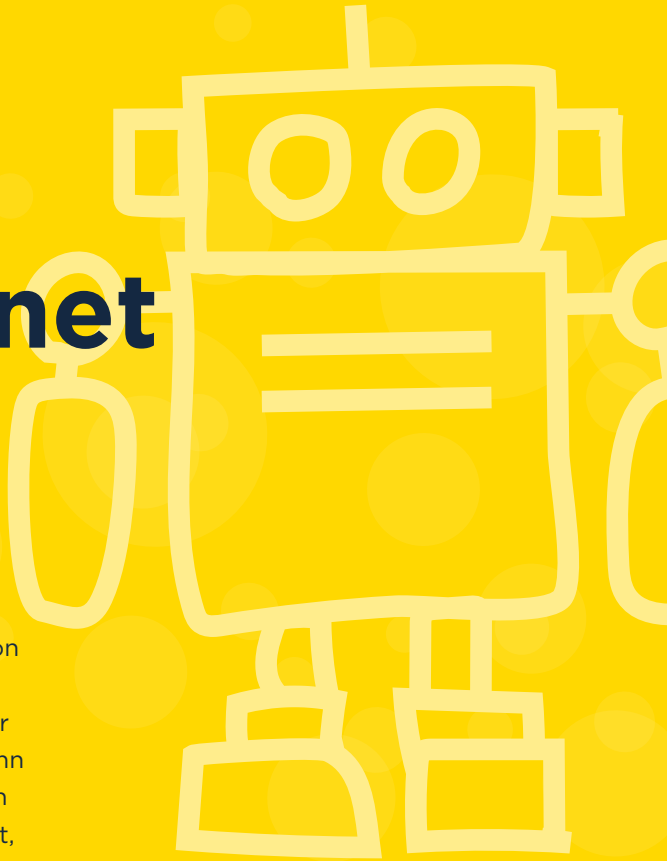
SPAMHAUS



Spamhaus Botnet Threat Update

Q1-2021

Nach einem eher ruhigen Jahresende 2020 in der Botnet-Welt von Spamhaus ging es dort im ersten Quartal 2021 direkt wieder zur Sache. Eine der positivsten Entwicklungen war zweifellos, dass der Botnet Emotet im Januar unschädlich gemacht wurde. Doch wenn eine Malware vom Netz geht, ist die nächste nicht weit, wie schon der 24-prozentige Anstieg der Gesamtzahl der Botnet C&Cs zeigt, den die Spezialisten von Spamhaus beobachteten.

Willkommen beim Spamhaus Botnet Threat Update für das 1. Quartal 2021.

Was sind Botnet 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 und 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.

Im Blickpunkt

Auch nach Emotet reißt der Strom neuer Bedrohungen nicht ab

Im Januar 2021 führte eine internationale Koalition aus Behörden verschiedener Länder eine konzertierte globale Maßnahme gegen den berüchtigten Botnet Emotet durch. Die Vollzugsbehörden schalteten die von der Emotet-Bande genutzte Infrastruktur ab und ließen den gesamten Emotet-Botnet-Traffic ins Leere laufen.

Es sieht so aus, als wäre die Operation ein Erfolg gewesen. Es wurden in diesem Zusammenhang zwar keine Verhaftungen vorgenommen, doch der Botnet ist seit mehr als zwei Monaten inaktiv. Trotzdem befürchten die Experten aus dem Spamhaus Malware Lab, dass Emotet irgendwann wieder in Umlauf kommen wird.

In den vergangenen Jahren hat Emotet floriert und sich den zweifelhaften Ruf erworben, eine der gefährlichsten Online-Bedrohungen überhaupt zu sein. Kriminelle nutzten diesen Botnet dazu, sich Zugang zu Unternehmensnetzwerken zu verschaffen, um sich dann lateral darin zu bewegen und in vielen Fällen eine Verschlüsselung mit Ransomware einzuschleusen.

Leider kommt die Botnet-Welt nie zur Ruhe. Sobald ein Botnet beseitigt wird, rückt der nächste nach. Und so haben andere Botnet-Betreiber nur darauf gewartet, die von Emotet hinterlassene Lücke zu füllen.

In diesem Quartal verbreiteten Betrüger über Botnets wie IcedID, Dridex, Quakbot und TrickBot eine Flut an Spam-E-Mails mit bösartigen Dokumenten. Bei den meisten dieser Bedrohungen ist die Vorgehensweise ähnlich wie bei Emotet, d. h. man versucht, einen Fuß in die Tür der Unternehmensnetzwerke zu bekommen und diese mit Ransomware zu verschlüsseln.

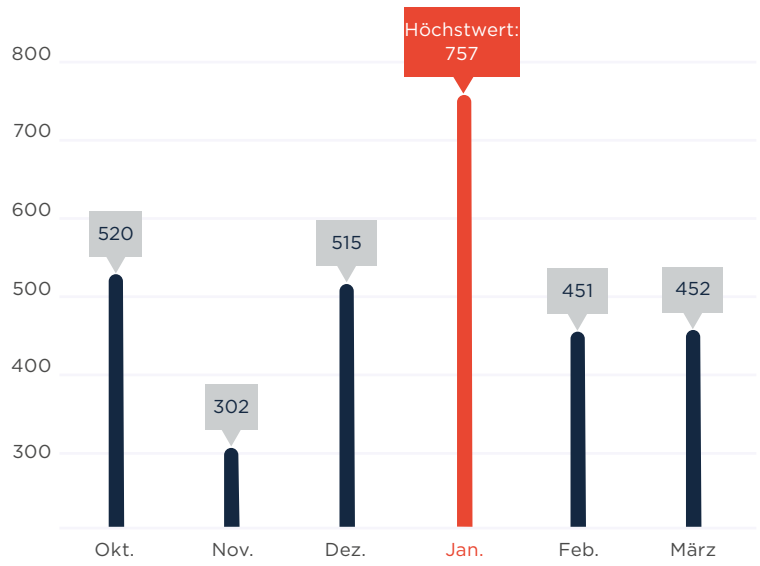
Emotet

Emotet ist ein ehemaliger E-Banking-Trojaner, der weltweit E-Banking-Kunden im Visier hatte. 2018 stellte Emotet seine betrügerischen E-Banking-Aktivitäten ein und begann damit, infizierten Computern ein „Pay-Per-Install"-Modell anzubieten. Ab 2019 entwickelte sich Emotet zu einem der gefährlichsten Botnets.

Anzahl der erkannten Botnet C&Cs, Q1-2021

Hier ist zunächst ein Überblick über die Anzahl der im 1. Quartal 2021 neu erkannten Botnet Command & Control Server (C&Cs). Spamhaus Malware Labs konnte im 1. Quartal 1.660 neue Botnet C&Cs identifizieren, im Vergleich zu 1.337 im 4. Quartal 2020. Dies ist ein Anstieg um 24 % mit durchschnittlich 553 Botnet C&Cs pro Monat.

Anzahl neuer Botnet C&Cs, die von Spamhaus seit Ende 2020 erkannt wurden:



Q4 Monatsdurchschnitt: 445

Q1 Monatsdurchschnitt: 553

Geografische Verteilung der Botnet C&C Hosts, Q1-2021

In einigen Ländern konnten wir einen Anstieg neu erkannter Botnet C&Cs beobachten, gleichzeitig fielen andere Länder aus unseren Top 20 heraus.

Die USA bleiben an der Spitze

Trotz eines geringfügigen Rückgangs der Anzahl neu erkannter Botnets von 3 % führen die USA die Rangliste weiter an.

Anstieg in Europa

Die Niederlande haben Russland überholt und liegen nun mit insgesamt 207 Botnets (27 % mehr als in Q4-2020) auf dem zweiten Platz.

Weitere europäische Länder haben Zunahmen an neuen Botnet-Infrastrukturen zu verzeichnen, z. B. Deutschland (+77 %), Frankreich (+82 %), die Schweiz (+23 %) und Großbritannien (+9 %).

Neuzugänge

Moldawien (11.), Hongkong (15.), Argentinien (18.), Kolumbien (18.).

Abgänge

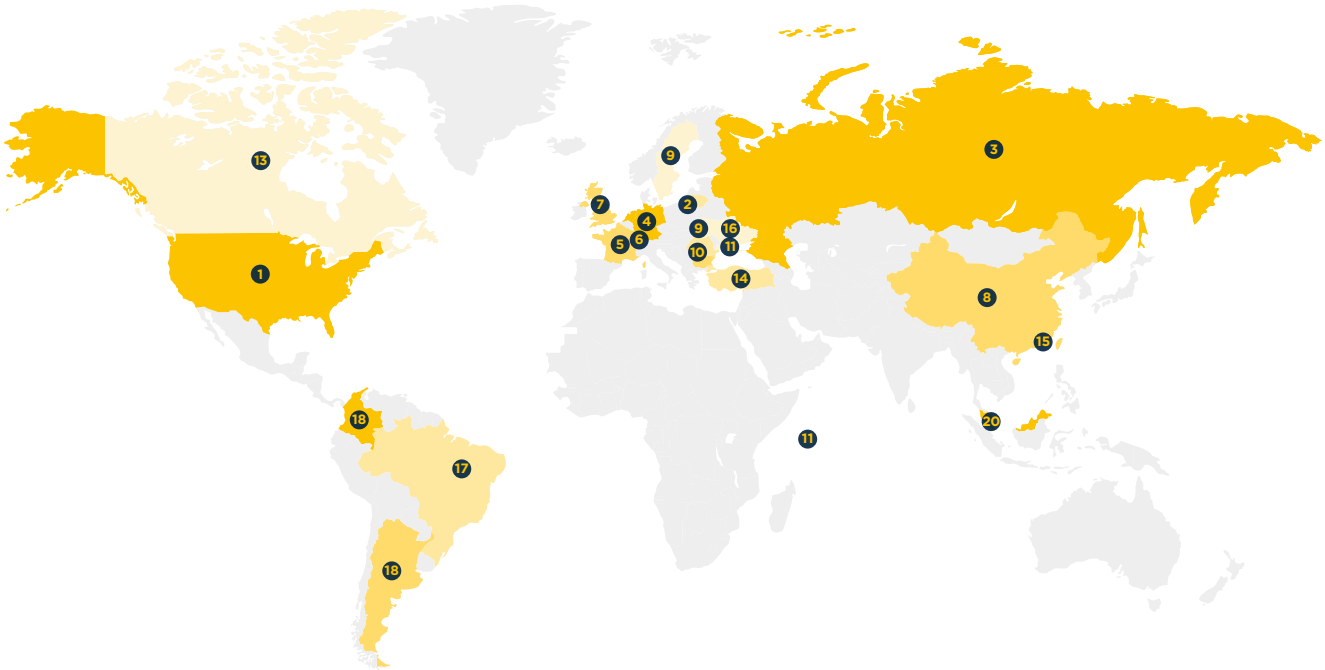
Bulgarien, Ungarn, Indien, Vietnam

Geografische Verteilung der Botnet C&Cs, Q1-2021 (Fortsetzung)

Top 20 Botnet C&C-Hosting-Länder

Rang	Land	Q4-2020	Q1-2021	% Veränderung gegenüber dem vorigen Quartal
1.	USA	348	338	-3 %
2.	Niederlande	163	207	27 %
3.	Russland	247	195	-21 %
4.	Deutschland	56	99	77 %
5.	Frankreich	39	71	82 %
6.	Schweiz	48	59	23 %
7.	Großbritannien	45	49	9 %
8.	China	32	42	31 %
9.	Schweden	34	39	15 %
10.	Lettland	24	31	29 %

Rang	Land	Q4-2020	Q1-2021	% Veränderung gegenüber dem vorigen Quartal
11.	Seychellen	10	29	190 %
11.	Moldawien	-	29	Neuzugang
13.	Kanada	11	25	136 %
14.	Türkei	17	20	47 %
15.	Hongkong	-	24	Neuzugang
16.	Ukraine	16	22	38 %
17.	Brasilien	8	20	150 %
18.	Argentinien	-	18	Neuzugang
18.	Kolumbien	-	18	Neuzugang
20.	Singapur	31	16	-48 %



SPAMHAUS

Mit Botnet C&Cs assoziierte Malware, Q1-2021

Emotet:

Im 1. Quartal 2021 sprang Emotet an die Spitze der Top 20. Das ist nicht überraschend – schließlich haben wir nicht umsonst den Vollzugsbehörden dabei geholfen, die Botnet-Infrastruktur von Emotet im Januar 2021 vom Netz zu nehmen.

Raccoon:

Raccoon ist ein neu aufgetretener Credential Stealer. Im 1. Quartal 2021 identifizierten wir 45 Botnet C&Cs, die mit dieser neuen Malware zusammenhingen.

FickerStealer:

Ein weiterer Credential Stealer, der im 1. Quartal 2021 erstmalig beobachtet wurde, ist FickerStealer, dem 25 neue Botnet C&Cs zugeordnet werden konnten.

QNodeService:

Dieser Malware beobachteten wir erstmalig im Jahr 2020. Es sieht jedoch so als, als wäre die Aktivität von QNodeService Anfang des Jahres komplett weggebrochen. Bis heute haben wir keinen einzigen damit zusammenhängenden C&C beobachtet.

Neuzugänge

Emotet (1.), Raccoon (8.), Gozi (10.), BitRat (12.), FickerStealer (15.), Vjw0rm (17.), TriumphLoader (17.), Hancitor (20.)

Abgänge

Mirai, QNodeService, BazaLoader, ZLoader, CobaltStrike, Smoke Loader, Dridex, RevengeRAT

Mit Botnet C&Cs assoziierte Malware, Q1-2021 (Fortsetzung)

Mit Botnet C&Cs assoziierte Malware-Familien

Rang	Q4-2020	Q1-2021	% Veränderung	Malware-Familie	Beschreibung
1.	–	272	Neuzugang	Emotet	Dropper
2.	53	124	134 %	RemcosRAT	Remote Access Tool (RAT)
3.	164	83	–49 %	Loki	Credential Stealer
4.	29	69	138 %	AsyncRAT	Remote Access Tool (RAT)
5.	71	68	–4 %	NanoCore	Remote Access Tool (RAT)
6.	66	55	–17 %	RedLine	Credential Stealer
6.	93	55	–41 %	AgentTesla	Remote Access Tool (RAT)
8.	–	45	Neuzugang	Raccoon	Credential Stealer
9.	17	39	129 %	Arkei	Credential Stealer
10.	–	38	Neuzugang	Gozi	E-Banking-Trojaner
11.	30	36	20 %	NjRAT	Remote Access Tool (RAT)
12.	21	33	57 %	NetWire	Remote Access Tool (RAT)
12.	–	33	Neuzugang	BitRAT	Remote Access Tool (RAT)
14.	38	30	–21 %	AveMaria	Remote Access Tool (RAT)
15.	–	25	Neuzugang	FickerStealer	Credential Stealer
16.	47	24	–49 %	AZORult	Credential Stealer
17.	15	18	20 %	QuasarRAT	Remote Access Tool (RAT)
17.	–	18	Neuzugang	Vjw0rm	Credential Stealer
17.	–	18	Neuzugang	TriumphLoader	Dropper
20.	–	17	Neuzugang	Hancitor	Dropper

Die am häufigsten missbrauchten Top Level Domains, Q1-2021

In Q1-2021 blieb die gTLD .com an der Spitze unserer Liste. Die meisten von Spamhaus Malware Labs identifizierten Botnet C&C-Domains wurden in dieser TLD gehostet. Erfreulich ist jedoch, dass viele andere gelistete TLDs ihren Ruf verbessern konnten.

.de:

Die deutsche ccTLD ist auf Rang 19 wieder in die Top 20 eingestiegen. Keine gute Entwicklung! Ist dies möglicherweise auf eine schwache Anti-Missbrauchsrichtlinie bei DENIC zurückzuführen?

.top und .xyz:

Diese beiden gTLDs haben eine lange Geschichte missbräuchlicher Nutzung. Daher überrascht es nicht, dass sie weiterhin in den Top 5 sind, besonders da bei .top die Zahl der gehosteten Botnet C&Cs im 1. Quartal 2021 um 90 % gestiegen ist.

Top Level Domains (TLDs) – eine Übersicht

Es gibt mehrere verschiedene Top Level Domains, darunter:

Generische TLDs (gTLDs) – 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) – unabhängige Top Level Domains, die nicht der Kontrolle der ICANN unterliegen

Neuzugänge

ru (6.), org (10.), biz (12.), us (15.), info (18.), co (19.), de (19.)

Abgänge

casa, br, cyou, kr, ai, ac, gq

Die am häufigsten missbrauchten Top Level Domains, Q1-2021 (Fortsetzung)

Mit Botnet C&Cs assoziierte Malware-Familien

Rang	Q4-2020	Q1-2021	% Veränderung	TLD	Typ
1.	2108	1549	-27 %	com	gTLD
2.	328	622	90 %	top	gTLD
3.	505	345	-32 %	xyz	gTLD
4.	141	124	-12 %	tk	Ursprünglich ccTLD, jetzt effektiv gTLD
5.	185	121	-35 %	ga	Ursprünglich ccTLD, jetzt effektiv gTLD
6.	-	114	Neuzugang	ru	ccTLD
7.	100	108	8 %	eu	ccTLD
8.	133	106	-20 %	ml	Ursprünglich ccTLD, jetzt effektiv gTLD
9.	95	87	-8 %	me	gTLD
10.	-	83	Neuzugang	org	gTLD
11.	94	82	-13 %	cf	Ursprünglich ccTLD, jetzt effektiv gTLD
12.	-	72	Neuzugang	biz	gTLD
12.	81	72	-11 %	net	gTLD
14.	138	66	-52 %	cc	gTLD
15.	-	55	Neuzugang	us	ccTLD
16.	77	51	-34 %	su	ccTLD
17.	74	47	-36 %	la	ccTLD
18.	-	46	Neuzugang	info	gTLD
19.	-	36	Neuzugang	co	ccTLD
19.	-	36	Neuzugang	de	ccTLD

Am häufigsten missbrauchte Domain-Registrierungsstellen, Q1-2021

Namecheap (schon wieder!)

Nach Jahren an der Spitze der Top 20 ist Namecheap (USA) weiterhin die bevorzugte Domain-Registrierungsstelle für Cyberkriminelle, die Botnet C&C-Domains registrieren lassen.

Wird sich das je ändern? Wir wissen es nicht. Doch in Anbetracht der langen Missbrauchsgeschichte bei Namecheap erwarten wir es nicht allzu bald!

Eranet International und RegRU

Mit einem massiven Anstieg von 249 % hat Eranet International (China) NameSilo (USA) von Platz 2 verdrängt. Den deutlichsten Anstieg der Botnet C&C-Domain-Registrierungen verzeichnet jedoch RegRU (Russland) mit sage und schreibe 341 %.

Neuzugänge

OnlineNIC (13.), name.com (15.), HiChina (16.), NameBright (17.)

Abgänge

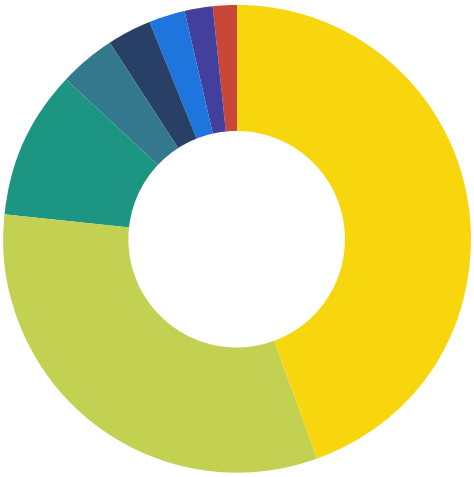
URL Solution, Hosting Concepts

Am häufigsten missbrauchte Domain-Registrierungsstellen, Q1-2021 (Fortsetzung)

Am häufigsten missbrauchte Domain-Registrierungsstellen – Anzahl der Domains

Rang	Q4-2020	Q1-2021	% Veränderung	Registrierungsstelle	Land
1.	822	628	-24 %	Namecheap	USA
2.	110	384	249 %	Eranet International	China
3.	444	259	-42 %	NameSilo	USA
4.	54	238	341 %	RegRU	Russland
5.	115	116	1 %	55hl.com	China
6.	101	85	-16 %	Alibaba	China
7.	343	72	-79%	PDR	Indien
8.	367	59	-84 %	Key Systems	Deutschland
9.	111	56	-50%	WebNic.cc	Singapur
10.	65	50	-23 %	west263.com	China
11.	25	44	76 %	101Domain	Irland
12.	48	42	-13 %	Bizcn	China
13.	-	38	Neuzugang	OnlineNIC	USA
14.	32	36	13 %	OVH	Frankreich
15.	-	35	Neuzugang	name.com	USA
16.	-	33	Neuzugang	HiChina	China
17.	-	30	Neuzugang	NameBright	USA
18.	53	29	-45 %	Tucows	USA
19.	46	28	-39 %	1API	Deutschland
20.	29	26	-10%	22net	China

Standort der am häufigsten missbrauchten Domain-Registrierungsstellen



Land	Botnets	%
USA	1019	44,5 %
China	736	32,2 %
Russland	238	10,4 %
Deutschland	87	3,8 %
Indien	72	3,1 %
Singapur	56	2,4 %
Irland	44	1,9 %
Frankreich	36	1,6 %

Netzwerke, welche die meisten neu erkannten Botnet C&Cs hosten, Q1-2021

In diesem Quartal waren gegenläufige Entwicklungen in Ost und West zu verzeichnen. Während sich bei den östlichen Providern die Zahl der gehosteten Botnet C&Cs verringerte, legten die westlichen Cloud-Serviceprovider in gleichem Maße zu.

Russische VPS-Provider (Virtual Private Server)

Verschiedene Firmen wie invs.ru und selectel.ru verschwanden in diesem Quartal aus den Top 20. Dies ist eine sehr positive Entwicklung insbesondere bei selectel.ru, die lange Zeit in den Top 20 vertreten waren.

Westliche VPS-Provider

Dafür sind viele im Westen ansässige Provider in Q1-2021 in die Top 20 aufgestiegen, darunter google.com, choopa.com, hetzner.de und combahton.net.

Die größten Verschlechterungen und Verbesserungen

Das am stärksten missbräuchlich genutzte Netzwerk ist privacyfirst.sh, ein VPN-Provider mit Sitz in Deutschland. Dahingegen sank im Netzwerk von amazon.com die Zahl der neu erkannten Botnet C&Cs gegenüber dem vorigen Quartal um 44 %. Auf jeden Fall ein Schritt in die richtige Richtung!

Neuzugänge

Google.com (2.), intersect.host (6.), choopa.com (12.) hetzner.de (13.), combahton.net (13.), linode.com (16.), ispserver.com (17.), colocrossing.com (17.), msk.host (17.)

Abgänge

invs.ru, m247.ro, selectel.ru, namecheap.com, digitalocean.com, maxko.org, tencent.com, baxet.ru, belcloud.net

[2] https://www.spamhaus.org/statistics/networks/

Netzwerke, welche die meisten neu erkannten Botnet C&Cs hosten, Q1-2021 (Fortsetzung)

Neu erkannte Botnet C&Cs pro Netzwerk

Rang	Q4-2020	Q1-2021	% Veränderung	Netzwerk	Land
1.	106	131	24 %	privacyfirst.sh	Deutschland
2.	–	53	Neuzugang	google.com	USA
3.	33	51	55 %	ovh.com	Frankreich
4.	47	45	-4 %	cloudflare.com	USA
5.	15	35	133 %	pq.hosting	Moldawien
6.	–	32	Neuzugang	intersect.host	Seychellen
7.	55	31	-44 %	amazon.com	USA
8.	45	28	-38 %	endurance.com	USA
9.	26	26	0 %	alibaba-inc.com	China
10.	15	23	53 %	itldc.com	Ukraine
11.	17	21	24 %	serverion.com	Niederlande
12.	–	20	Neuzugang	choopa.com	USA
13.	–	19	Neuzugang	hetzner.de	Deutschland
13.	–	19	Neuzugang	combahton.net	Deutschland
13.	28	19	-32 %	leaseweb.com	Niederlande
16.	–	18	Neuzugang	linode.com	USA
17.	–	17	Neuzugang	ispserver.com	Russland
17.	–	17	Neuzugang	colocrossing.com	USA
17.	25	17	-32 %	dedipath.com	USA
17.	–	17	Neuzugang	msk.host	Russland

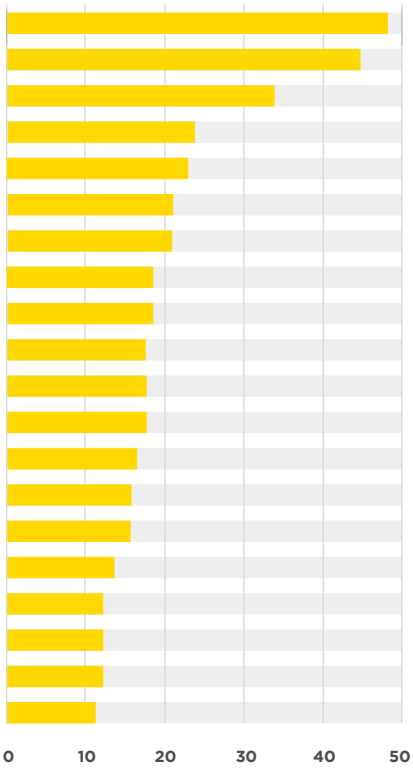
Netzwerke, welche die aktivsten Botnet C&Cs hosten, Q1-2021

Zum guten Schluss sehen wir uns die Netzwerke an, die kontinuierlich eine große Zahl aktiver Botnet C&Cs gehostet haben. Leider führt Microsoft diese Top 20 mit 48 aktiven Botnet C&Cs an, gefolgt von Google mit 43.

Die in dieser Liste aufgeführten Netzwerke haben in der Regel eine schlechte Netzwerkhygiene und versäumen es, bei Beschwerden über missbräuchliche Nutzung Maßnahmen zu ergreifen – darauf weist zumindest die mangelnde Veränderung in den vergangenen Quartalen hin. Die Botnets bleiben monatelang aktiv!

Gesamtzahl aktiver Botnet C&Cs pro Netzwerk

Rang	Q4-2020	Q1-2021	% Veränderung	Netzwerk	Land
1.	48	48	0 %	microsoft.com	USA
2.	43	43	0 %	google.com	USA
3.	33	33	0 %	ipjetable.net	Schweiz
4.	23	23	0 %	ttnet.com.tr	Türkei
5.	22	22	0 %	charter.com	USA
6.	21	21	0 %	inmotionhosting.com	USA
6.	21	21	0 %	vietserver.vn	Vietnam
8.	18	18	0 %	claro.com.co	Kolumbien
8.	18	18	0 %	cloudvider.net	Großbritannien
10.	17	17	0 %	ovpn.com	Schweden
10.	17	17	0 %	une.net.co	Kolumbien
10.	17	17	0 %	datawire.ch	Schweiz
13.	16	16	0 %	mail.ru	Russland
14.	14	14	0 %	chinanet-js	China
14.	14	14	0 %	digitalocean.com	USA
16.	13	13	0 %	mtnnigeria.net	Nigeria
17.	12	12	0 %	kornet.net	Korea
17.	12	12	0 %	hostry.com	Zypern
19.	12	11	-8 %	eurobyte.ru	Russland
19.	11	11	0 %	telstra.com	Australien



Angesichts der Ereignisse im Zusammenhang mit Emotet im 1. Quartal 2021 wird es äußerst interessant sein zu beobachten, was die nahe Zukunft bringen wird.

Bis zum nächsten Quartal. Bleiben Sie gesund.