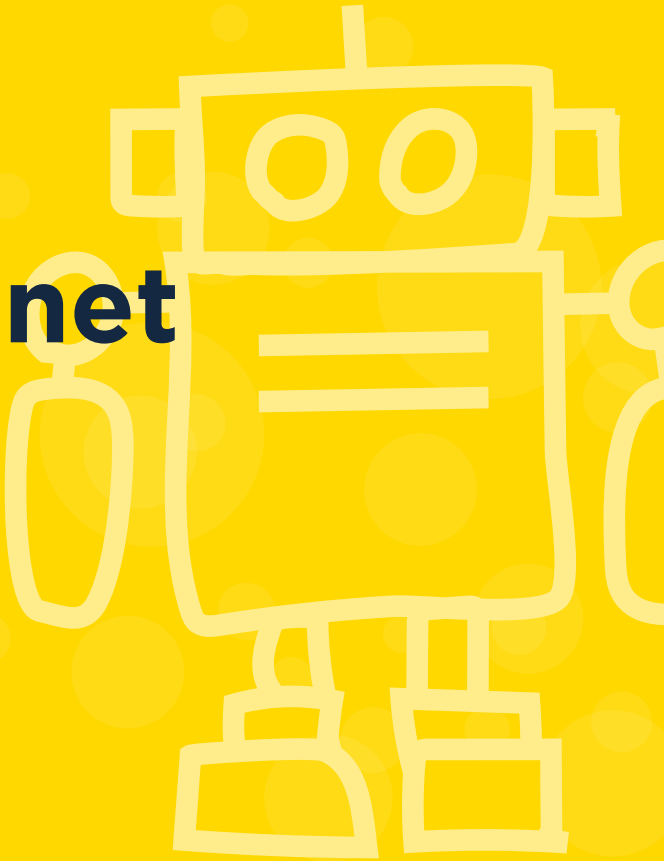
Spamhaus Botnet Threat Update



Q2-2021

In diesem Quartal haben die Recherchespezialisten von Spamhaus bei neu erkannten Botnet Command-and-Controllers (C&Cs) einen Rückgang von 12 % beobachtet – eine gute Nachricht. Allerdings nicht für alle. Mehr als ein branchenführender Provider ächzt unter dem Gewicht der aktiven Botnet C&Cs in seinem Netzwerk.

Willkommen beim Spamhaus Botnet Threat Update für das 2. 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 so personenbezogene oder 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

Die unendliche Geschichte von Emotet

Ja, wir wissen es – wir reden hier über Emotet, obwohl die Schadsoftware schon im Januar vom Netz genommen wurde. Doch damit ist die Geschichte von Emotet noch nicht zu Ende. Noch lange nicht.

Wegen der Art und Weise, in der sich Emotet verbreitet hat, d. h. durch Thread Hijacking, wurden Millionen von E-Mail-Konten beeinträchtigt. Damit waren Tür und Tor für den weiteren Missbrauch durch andere Malware und Ransomware geöffnet.

Spamhaus hat die letzten drei Monate mit dem FBI zusammengearbeitet, um zur Bewältigung der Krise beizutragen und den Betroffenen zu helfen. Hier einige Zahlen, um die Größenordnung des Problems fassbar zu machen:

- 1,3 Millionen beeinträchtigte E-Mail-Konten
- 22.000 einzelne Domains
- 3.000 Netzwerke

Unser Team arbeitet mit Hochdruck daran, mit den zuständigen Meldestellen und Sicherheitsabteilungen sowie Endnutzern Kontakt aufzunehmen, um ihnen Daten und Anleitungen für die Problembehebung zur Verfügung zu stellen, mit denen sie ihre beeinträchtigten Konten schützen können.

Wir sind froh, dass mittlerweile über 60 % dieser 1,3 Millionen Konten gesichert werden konnten. Daran wird deutlich, dass wir alle dazu beitragen müssen, das Internet sicherer zu machen.

Was ist Thread Hijacking?

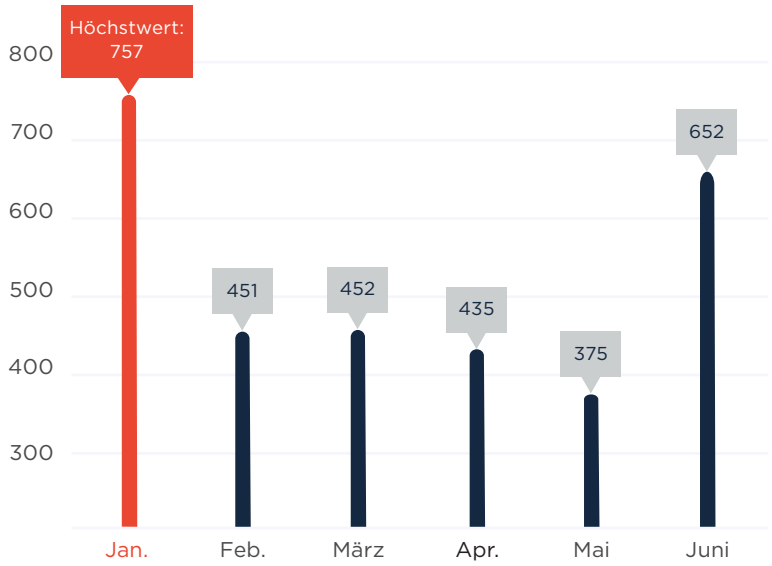
Beim Thread Hijacking nutzen Betrüger bestehende E-Mail-Konversationen (Threads) Ihrer Opfer, um bösartige Links oder Anhänge an neue Opfer zu versenden.

Dadurch wirkt ein Angreifer weitaus überzeugender und kann weitere Opfer dazu verleiten, auf schädliche Links zu klicken oder Dateien herunterzuladen, da Betroffenen den Eindruck haben, auf einen bestehenden E-Mail-Thread zu antworten.

Anzahl der erkannten Botnet C&Cs, Q2-2021

Hier ist ein Überblick über die Anzahl der im 2. Quartal 2021 neu erkannten Botnet Command & Control Server (C&Cs). Spamhaus Malware Labs konnten im 2. Quartal **1.462 Botnet C&Cs** identifizieren, im Vergleich zu 1.660 im 1. Quartal 2021. Dies stellt einen **Rückgang** von **12 %** dar. Der Monatsdurchschnitt sank von 553 in Q1 auf 487 Botnet C&Cs in Q2.

Anzahl der von Spamhaus 2021 neu erkannten Botnet C&Cs:



Q1 Monatsdurchschnitt: 553

Q2 Monatsdurchschnitt: 487

Geografische Verteilung der Botnet C&C Hosts, Q2-2021

Die geografischen Orte, an denen Cyberkriminelle neue Botnet C&C-Server eingerichtet haben, hat sich vor allem bei den Top 20 mehrfach geändert, mit einer großen Zahl an Neuzugängen.

Rückläufige Zahlen in Lateinamerika

In den lateinamerikanischen Ländern war ein merklicher Rückgang bei Botnet C&Cs zu verzeichnen. Argentinien und Kolumbien fielen aus der Liste der Top 20 Hosts heraus, Brasilien verzeichnete einen Rückgang von 40 %. Die einzige Ausnahme war Panama, das auf Rang 13 neu in die Liste einstieg.

Kontinuierlicher Anstieg in Europa

Erneut war ein Anstieg der Zahl der europäischen Länder zu beobachten, die in die Top 20 aufstiegen. Hierzu zählten beispielsweise die Tschechische Republik, Polen und Finnland. Gleichzeitig nahm auch in Ländern wie Deutschland, Frankreich, Lettland und Großbritannien die Zahl der Botnet C&Cs zu.

Neuzugänge

Tschechische Republik (11.), Panama (13.), Malaysia (15.), Polen (15.), Finnland (17.), Vietnam (18.).

Abgänge

China, Schweden, Hongkong, Argentinien, Kolumbien, Singapur.

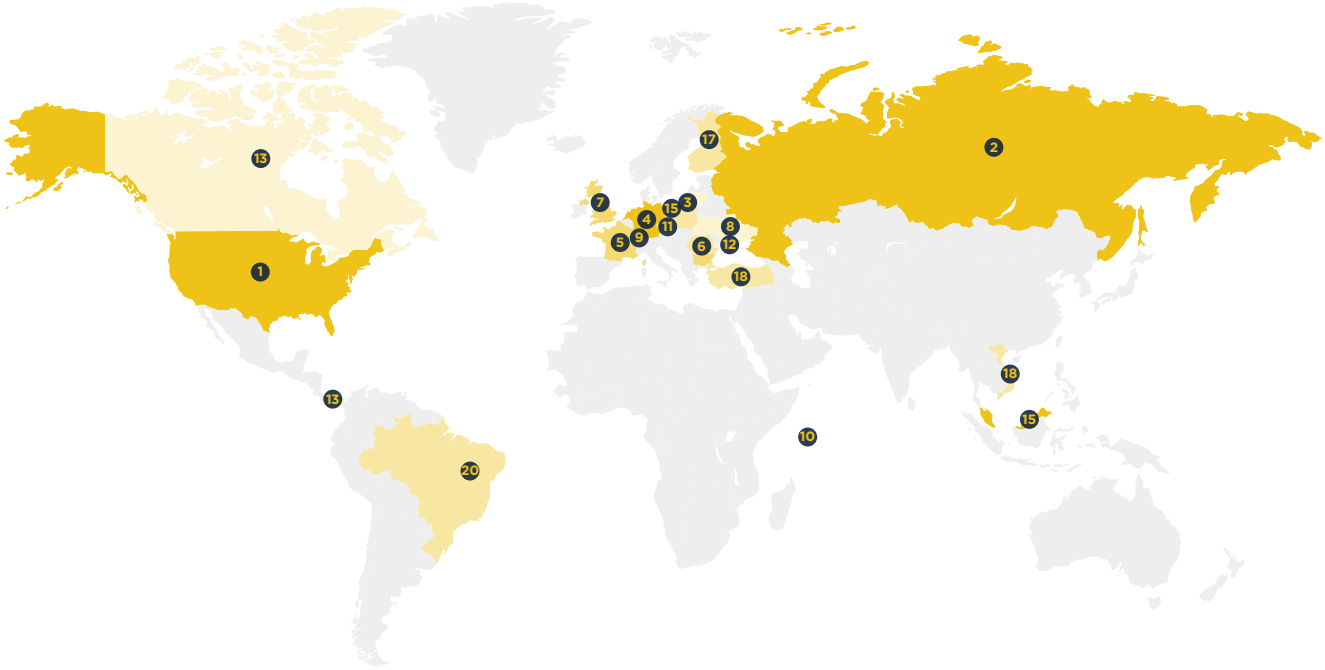
Geografische Verteilung der Botnet C&C Hosts, Q2-2021 (Fortsetzung)

Top 20 Botnet C&C-Hosting-Länder

Rang	Land	Q1 2021	Q2 2021	% Veränderung gegenüber dem vorigen Quartal
1.	USA	338	281	-17 %
2.	Russland	195	233	19 %
3.	Niederlande	207	168	-19 %
4.	Deutschland	99	117	18 %
5.	Frankreich	71	92	30 %
6.	Lettland	31	84	171 %
7.	Großbritannien	49	57	16 %
8.	Ukraine	22	44	100 %
9.	Schweiz	59	41	-31 %
10.	Seychellen	29	38	31 %

Neuzugang

Rang	Land	Q1 2021	Q2 2021	% Veränderung gegenüber dem vorigen Quartal
11.	Tschechische Republik	-	31	Neuzugang
12.	Moldawien	29	29	0 %
13.	Panama	-	16	Neuzugang
13.	Kanada	26	16	-38 %
15.	Malaysia	-	15	Neuzugang
15.	Polen	-	15	Neuzugang
17.	Finnland	-	14	Neuzugang
18.	Vietnam	-	13	Neuzugang
18.	Türkei	25	13	-48 %
20.	Brasilien	20	12	-40 %



Mit Botnet C&Cs assoziierte Malware, Q2-2021

Beginnen wir mit der guten Nachricht. Nachdem der Emotet-Botnet im ersten Quartal 2021 vom Netz genommen wurde, können wir erfreulicherweise berichten, dass von Emotet keine weitere Aktivität ausging.

Dropper immer beliebter

Im 2. Quartal gab es eine Verschiebung von Credential Stealers und Remote Access Tools (RATs) hin zu Droppers.

Raccoon schnell auf Platz 1

Raccoon ist erst seit dem letzten Quartal in den Top 20 vertreten, als der Stealer auf Rang 8 in die Liste einstieg, um nun im 2. Quartal die Führung zu übernehmen.

Credential Stealers zu verkaufen

Nicht nur dieser Credential Stealer Raccoon wird mittlerweile im Dark Web zum Verkauf angeboten, auch ähnliche Stealer wie RedLine und Oski, die es in diesem Quartal erstmals in unsere Charts schafften, sind dort vertreten. Angesichts des einfachen Zugriffs ist es nicht weiter überraschend, dass solche Malware sich zunehmender Beliebtheit erfreut.

Was ist ein Dropper?

Dropper versuchen mit getarntem Code zu erreichen, dass Malware der Entdeckung durch Virenscanner entgeht, d. h. sie legen die Malware „geräuschlos“ im avisierten System ab.

Neuzugänge

Oski (7.), Tofsee (11.), STRRAT (15.), CryptBot (16.), CobaltStrike (17.), ServHelper (18.), IcedID (18.).

Abgänge

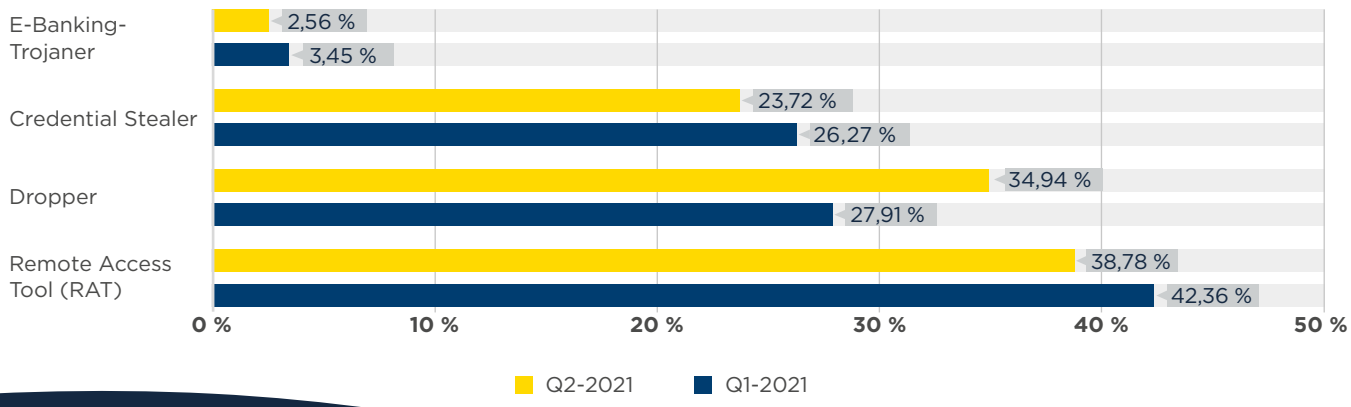
Emotet, NetWire, AveMaria, FickerStealer, AZORult, TriumpLoader, Hancitor

Mit Botnet C&Cs assoziierte Malware, Q2-2021 (Fortsetzung)

Mit Botnet C&Cs assoziierte Malware-Familien

Rang	Q1-2021	Q2-2021	% Veränderung	Malware-Familie	Beschreibung
1.	45	302	571 %	Raccoon	Dropper
2.	55	123	124 %	RedLine	Remote Access Tool (RAT)
3.	69	83	20 %	AsyncRAT	Credential Stealer
4.	83	66	-20 %	Loki	Remote Access Tool (RAT)
5.	38	43	13 %	Gozi	Remote Access Tool (RAT)
6.	33	42	27 %	BitRAT	Credential Stealer
7.	-	28	Neuzugang	Oski	Remote Access Tool (RAT)
8.	18	26	44 %	Vjw0rm	Credential Stealer
9.	36	24	-33 %	NjRAT	Credential Stealer
9.	124	24	-81 %	RemcosRAT	E-Banking-Trojaner
11.	68	23	-66 %	NanoCore	Remote Access Tool (RAT)
11.	55	23	-58 %	AgentTesla	Remote Access Tool (RAT)
11.	-	23	Neuzugang	Tofsee	Remote Access Tool (RAT)
14.	39	19	-51 %	Arkei	Remote Access Tool (RAT)
15.	-	17	Neuzugang	STRRAT	Credential Stealer
16.	-	16	Neuzugang	CryptBot	Credential Stealer
17.	-	15	Neuzugang	CobaltStrike	Remote Access Tool (RAT)
18.	-	14	Neuzugang	ServHelper	Credential Stealer
18.	-	14	Neuzugang	IcedID	Dropper
20.	18	11	-39 %	QuasarRAT	Dropper

Vergleich der Malware-Typen zwischen Q1-und Q2-2021



Die am häufigsten missbrauchten Top Level Domains, Q2-2021

.com

In Q2-2021 schaffte es die gTLD .com erneut an die Spitze unserer Liste. Darüber hinaus stieg die Zahl der neu registrierten Botnet C&C Domains auf .com um 166 %, nämlich von 1.549 auf 4.113!

.xyz

In Anbetracht des gewaltigen Anstiegs um 114 % in diesem Quartal ist es nicht weiter überraschend, dass die gTLD .xyz die gTLD .top auf dem 2. Rang abgelöst hat.

Länderspezifische TLD

Nur zwei neue ccTLDs schafften es dieses Quartal unter die Top 20, nämlich .br auf Nr. 5 und .cn auf Nr. 12. Zwischenzeitlich haben drei ccTLDs ihren Ruf verbessert und konnten die Liste verlassen, nämlich .us, .de und .la.

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

buzz (3.), br (5.), VIP (6.), cloud (10.), cn (12.), online (16.), live (17.).

Abgänge

me, biz, cc, us, la, co, de.

Die am häufigsten missbrauchten Top Level Domains, Q2-2021 (Fortsetzung)

Die am häufigsten missbrauchten TLDs – Anzahl der Domains

Rang	Q1-2021	Q2-2021	% Veränderung	TLD	Typ
1.	1549	4113	166 %	com	gTLD
2.	345	739	114 %	xyz	gTLD
3.	-	662	Neuzugang	buzz	gTLD
4.	622	607	-2 %	top	gTLD
5.	-	208	Neuzugang	br	ccTLD
6.	-	175	Neuzugang	vip	gTLD
7.	83	157	89 %	org	gTLD
8.	114	151	32 %	ru	ccTLD
9.	72	146	103 %	net	gTLD
10.	-	141	Neuzugang	cloud	gTLD
11.	124	140	13 %	tk	Ursprünglich ccTLD, jetzt effektiv gTLD
12.	-	139	Neuzugang	cn	ccTLD
12.	108	116	7 %	eu	ccTLD
14.	121	106	-12 %	ga	Ursprünglich ccTLD, jetzt effektiv gTLD
15.	106	104	-2 %	ml	Ursprünglich ccTLD, jetzt effektiv gTLD
16.	-	86	Neuzugang	online	gTLD
17.	-	81	Neuzugang	live	gTLD
18.	51	80	57 %	su	ccTLD
19.	46	78	70 %	info	gTLD
20.	82	73	-11 %	cf	ccTLD

Am häufigsten missbrauchte Domain-Registrierungsstellen, Q2-2021

Nach vielen Jahren ohne Veränderung an der Spitze unserer Reputationsrangliste der Registrierungsstellen gibt es nun Bewegung zu vermelden!

NameSilo

Wir konnten einen gewaltigen Anstieg von 594 % bei neu registrierten Botnet C&C Domains bei der US-amerikanischen Registrierungsstelle NameSilo beobachten, die der bisherigen Nr. 1 Namecheap den Spitzenplatz streitig machte. Eine echte Leistung angesichts der Tatsache, dass Namecheap einen Zuwachs von 52 % an neu registrierten Botnet C&C Domains verzeichnen konnte. Gewaltige Zahlen!

Deutschland und China

Doch nicht nur US-amerikanische Registrierungsstellen hatten im 2. Quartal beträchtliche Zuwächse zu vermelden. Die beiden in Deutschland ansässigen Registrierungsstellen Key Systems (56 %) und 1API (254 %) hatten ebenfalls eine Zunahme der über ihre Dienste registrierten Botnet Domains zu verzeichnen, wie auch die unten aufgeführten chinesischen Registrierungsstellen wie eName Technology, ein Neuzugang an Nr. 3.

Neuzugänge

eName Technology (3.), Arsys (5.), Xin Net (10.), CentralNic (11.), Network Solutions (14.).

Abgänge

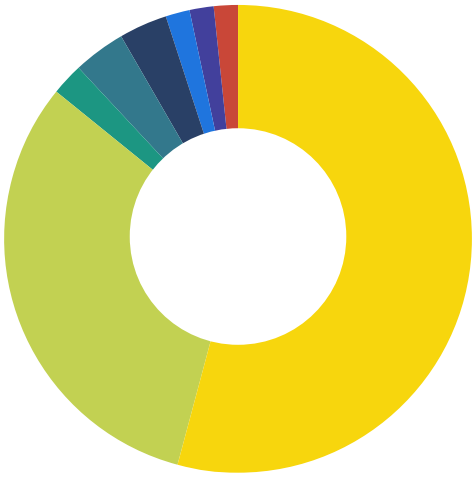
101 Domains, Bizcn, OnlineNIC, OVH, NameBright.

Am häufigsten missbrauchte Domain-Registrierungsstellen, Q2 2021 (Fortsetzung)

Am häufigsten missbrauchte Domain-Registrierungsstellen – Anzahl der Domains

Rang	Q1-2021	Q2-2021	% Veränderung	Registrierungsstellen	Land
1.	259	1797	594 %	NameSilo	USA
2.	628	955	52 %	Namecheap	USA
3.	-	526	Neuzugang	eName Technology	China
4.	85	504	493 %	Alibaba	China
5.	-	237	Neuzugang	Arsys	Spanien
6.	384	215	-44 %	Eranet International	China
7.	72	188	161 %	PDR	Indien
8.	238	135	-43 %	RegRU	Russland
9.	33	134	306 %	HiChina	China
10.	-	125	Neuzugang	Xin Net	China
11.	-	112	Neuzugang	CentralNic	Großbritannien
12.	26	110	323 %	22net	China
12.	29	110	279 %	Tucows	USA
14.	-	101	Neuzugang	Network Solutions	USA
15.	28	99	254 %	1API	Deutschland
16.	59	92	56 %	Key Systems	Deutschland
17.	56	91	63 %	WebNic.cc	Singapur
18.	35	89	154 %	Name.com	USA
19.	50	80	60 %	west263.com	China
20.	116	73	-37 %	55hl.com	China

STANDORT DER AM HÄUFIGSTEN MISSBRAUCHTEN DOMAIN-REGISTRIERUNGSSTELLEN



Land	Botnets	%
USA	3052	52,9 %
China	1767	30,6 %
Spanien	237	2,3 %
Deutschland	191	3,3 %
Indien	188	3,3 %
Russland	135	1,6 %
Großbritannien	112	1,6 %
Singapur	91	1,6 %
Gesamt	5773	

Netzwerke, welche die meisten neu erkannten Botnet C&Cs hosten, Q2-2021

Bei den Netzwerken, welche die meisten neu erkannten Botnet C&Cs hosten, ist immer viel Bewegung. Das 2. Quartal ist da keine Ausnahme.

Bulletproof Hosting

Im 2. Quartal zog einer der größten Bulletproof-Hosting-Betriebe von Amazon zu DigitalOcean um. Infolge dessen sank die Anzahl neu beobachteter Botnet C&Cs bei Amazon drastisch. Im Gegensatz dazu gab es einen plötzlichen Anstieg neuer Botnet C&Cs bei DigitalOcean zu verzeichnen.

Microsoft.com

Wir konnten beobachten, wie microsoft.com (US) in die Top 20 aufstieg. Wir konnten auch sehen, wie dort eine beträchtliche Anzahl von Vjw0rm und BitRAT Botnet C&C-Infrastrukturen aus dem Boden wuchsen.

Neuzugänge

nano.lv (6.), mgnhost.ru (8.), baxet.ru (10.), ipjetable.net (11.), digitalocean.com (12.), internet.it (14.), hostsailor.com (16.), microsoft.com (17.), m247.ro (8.), offshoreracks.com (19.), mivocloud.com (19.).

Abgänge

intersec.host, amazon.com, endurance.com, choopa.com, combahton.net, leaseweb.com, linode.com, ispserver.com colocrossing.com, dedipath.com, msk.host.

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

Netzwerke, welche die meisten neu erkannten Botnet C&Cs hosten, Q2-2021 (Fortsetzung)

Neu erkannte Botnet C&Cs pro Netzwerk

Rang	Q1-2021	Q2-2021	% Veränderung	Netzwerk	Land
1.	35	82	134 %	pq.hosting	Russland
2.	53	74	40 %	google.com	USA
3.	21	68	224 %	serverion.com	Niederlande
4.	51	56	10 %	ovh.com	Frankreich
5.	23	53	130 %	itldc.com	Ukraine
6.	-	49	Neuzugang	nano.lv	Lettland
7.	131	48	-63 %	privacyfirst.sh	Deutschland
8.	-	47	Neuzugang	mgnhost.ru	Russland
9.	19	46	142 %	hetzner.de	Deutschland
10.	-	40	Neuzugang	baxet.ru	Russland
11.	-	35	Neuzugang	ipjetable.net	Frankreich
12.	45	29	-36 %	cloudflare.com	USA
12.	-	29	Neuzugang	digitalocean.com	USA
14.	-	28	Neuzugang	Internet.it	Russland
15.	26	26	0 %	alibaba-inc.com	China
16.	-	25	Neuzugang	hostsailor.com	Verein. Arab. Emirate
17.	-	22	Neuzugang	microsoft.com	USA
18.	-	21	Neuzugang	m247.ro	Rumänien
19.	-	16	Neuzugang	offshoreracks.com	Panama
19.	-	16	Neuzugang	mivocloud.com	Moldawien

Netzwerke, welche die aktivsten Botnet C&Cs hosten, Q2-2021

Zum guten Schluss sehen wir uns die Netzwerke an, die im 2. Quartal 2021 eine große Zahl aktiver Botnet C&Cs gehostet haben. Hosting-Provider, die in dieser Rangliste erscheinen, haben entweder ein Missbrauchsproblem oder sie treffen keine geeigneten Maßnahmen, wenn sie Meldungen über missbräuchliche Nutzungen erhalten.

Neuzugänge

m247.ro (12.), eliteteam.to (13.), mgnhost.ru (13.), unusinc.com (17.).

Abgänge

mail.ru, digitalocean.com, eurobyte.ru, telstra.com.

Eliteteam.to

Dies ist ein Bulletproof-Hosting-Unternehmen, das angeblich auf den Seychellen ansässig ist. Tatsächlich sieht es eher danach aus, dass sie von Russland aus operiert.

Microsoft.com und google.com

Es ist offensichtlich, dass Microsoft mit der großen Zahl missbräuchlicher Nutzungen seiner Cloud-Plattform Azure zu kämpfen hat. Auch google.com wird praktisch mit Missbrauchsmeldungen überschüttet.

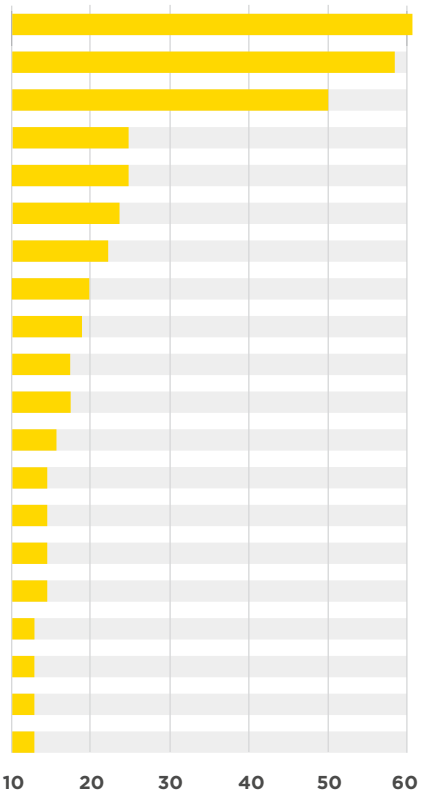
Glückwunsch den Abgängen!

Wir gratulieren all denjenigen, die sich aus dieser Liste verabschieden konnten – gut, dass die Zahl der aktiven Botnet C&Cs in Ihrem Netzwerk abnimmt. Gute Arbeit!

Netzwerke, welche die aktivsten Botnet C&Cs hosten, Q2-2021 (Fortsetzung)

Gesamtzahl aktiver Botnet C&Cs pro Netzwerk

Rang	Q4 2020	Q1-2021	% Veränderung	Netzwerk	Land
1.	33	61	85 %	ipjetable.net	Frankreich
2.	48	58	21 %	microsoft.com	USA
3.	43	50	16 %	google.com	USA
4.	23	23	0 %	ttnet.com.tr	Türkei
4.	21	23	10 %	vietserver.vn	Vietnam
6.	22	21	-5 %	charter.com	USA
6.	21	21	0 %	inmotionhosting.com	USA
8.	17	20	18 %	ovpn.com	Schweden
9.	18	18	0 %	clouvider.net	Großbritannien
10.	12	17	42 %	hostry.com	Zypern
10.	17	17	0 %	une.net.co	Kolumbien
12.	-	15	Neuzugang	m247.ro	Rumänien
13.	17	13	-24 %	datawire.ch	Schweiz
13.	-	13	Neuzugang	eliteteam.to	Seychellen
13.	13	13	0 %	mtnnigeria.net	Nigeria
13.	-	13	Neuzugang	mgnhost.ru	Russland
17.	18	12	-33 %	claro.com.co	Kolumbien
17.	12	12	0 %	kornet.net	Südkorea
17.	14	12	-14 %	chinanet-js	China
17.	-	12	Neuzugang	unusinc.com	USA



Damit verabschieden wir uns für heute.

Im Oktober sehen wir uns wieder. Bleiben Sie gesund!