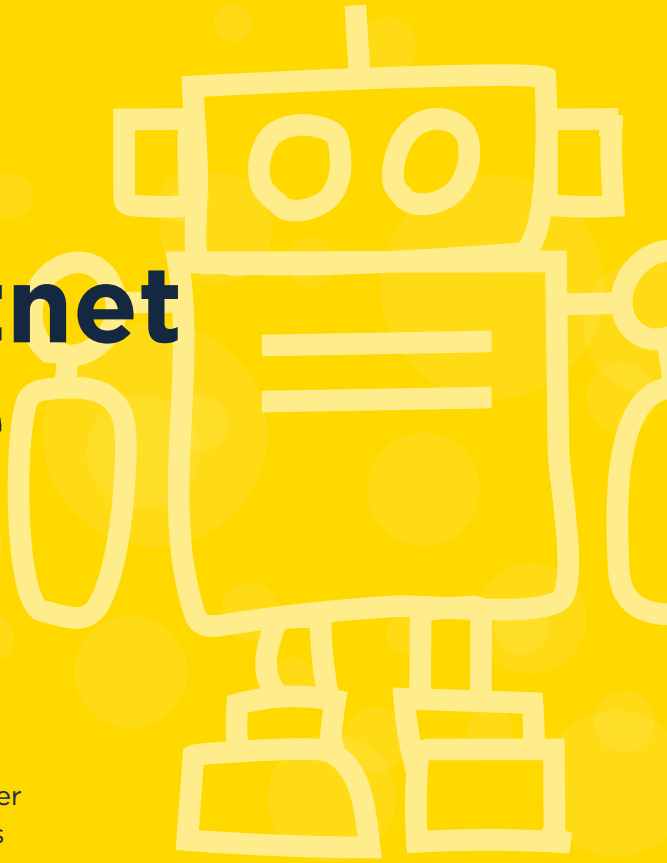
SPAMHAUS

Spamhaus Botnet Threat Update



Q3-2021

Im dritten Quartal stieg die Zahl der neuen von unserem Rechercheteam identifizierten Botnet Command & Controllers (C&Cs) um sage und schreibe 82 %. Man beobachtete eine explosionsartige Zunahme von Backdoor-Malware durch bösartige Betreiber, die sich hinter FastFlux verstecken. Dies hat wiederum dazu geführt, dass mehrere Länder und Dienstanbieter jetzt neu in unseren Top 20 gelistet sind.

Willkommen beim Spamhaus Botnet Threat Update für das 3. Quartal 2021.

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 werden.

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

FastFlux ist wieder da

Bei der Auswertung der statistischen Daten dieses Quartals wird deutlich, dass FastFlux wieder populärer geworden ist. Für alle, die sich nicht mehr ganz sicher sind, was FastFlux ist und wie Cyberkriminelle diesen Dienst dazu nutzen, ihre Infrastruktur gegen Außerbetriebnahmen zu schützen, haben wir die Fakten hier noch einmal zusammengefasst.

Was ist FastFlux?

FastFlux ist eine von Phishing-, Malware- und Botnet-Betreibern angewandte Technik, mit der sie den tatsächlichen Standort ihrer Infrastruktur hinter einem Netzwerk beeinträchtigter Hosts verbergen, die als Proxy fungieren und den bösartigen Verkehr an das tatsächliche Backend weiterleiten.

Warum ist FastFlux für Cyberkriminelle so attraktiv?

Alle FastFlux-Netzwerke, die zurzeit in Betrieb sind, können als Dienst im Darknet gemietet werden. Das macht Botnet-Betreibern das Leben leicht. Sie müssen lediglich noch die für ihre Botnet C&Cs benötigten Domains registrieren lassen und sie an den Dienst des FastFlux-Betreibers verweisen. FastFlux übernimmt den Rest und stellt sicher, dass sich die A-Records rasch ändern.

Hier ist ein Beispiel für eine FluBot-Botnet-C&C-Domain, die auf einem FastFlux-Botnet gehostet wird:

```
;; QUESTION SECTION:
;gurbngbcxheshsj.ru.       IN    A

;; ANSWER SECTION:
```

Domain	TTL	RecordType		IP Address
gurbngbcxheshsj.ru.	150	IN	A	189.165.94.67
gurbngbcxheshsj.ru.	150	IN	A	124.109.61.160
gurbngbcxheshsj.ru.	150	IN	A	187.190.48.60
gurbngbcxheshsj.ru.	150	IN	A	115.91.217.231
gurbngbcxheshsj.ru.	150	IN	A	175.126.109.15
gurbngbcxheshsj.ru.	150	IN	A	175.119.10.231
gurbngbcxheshsj.ru.	150	IN	A	218.38.155.210
gurbngbcxheshsj.ru.	150	IN	A	179.52.22.168
gurbngbcxheshsj.ru.	150	IN	A	113.11.118.155
gurbngbcxheshsj.ru.	150	IN	A	14.51.96.70

Wie Sie sehen, nutzt die Botnet C&C Domain gleichzeitig zehn A-Records mit einer „Time to live“ (TTL) von nur 150 Sekunden. Eine Überwachung dieser A-Records ergibt, dass der zugrunde liegende FastFlux-Botnet 100 bis 150 aktive FastFlux-Knoten pro Tag umfasst.

Generell handelt es sich bei diesen Knoten um beeinträchtigte Endgeräte beim Kunden (das sogenannte Customer Premise Equipment, CPE), die unzulänglich konfiguriert sind (d. h. mit anfälliger Software laufen oder Standardanmeldedaten verwenden) und direkt über das Internet zugänglich sind.

Diese Art von Geräten ist ein leichtes Ziel für Cyberkriminelle. Angreifer müssen nur internetweite Scans ausführen, um solche anfälligen Geräte zu entdecken und zu beeinträchtigen. Der gesamte Prozess kann automatisiert werden – schnell, einfach und effektiv.

Betreiber von FastFlux-Botnets gehen bei der Auswahl des geografischen Standorts der Geräte, die sie für das FastFlux-Hosting verwenden, sehr sorgsam vor. Wie Sie bei der Lektüre dieses Berichts feststellen werden, befinden sich die Hosts vieler FastFlux-C&C-Knoten an Orten, die relativ gut digitalisiert sind, d. h., die eine gute Internetverbindungen haben, deren Cybersicherheit aber noch nicht ganz so weit entwickelt ist.

Lateinamerika ist ein beliebtes Ziel, beispielsweise Brasilien, Chile, Argentinien, Uruguay, und auch asiatische Länder wie Korea. Die Neuzugänge in der Statistik der geografischen Standorte spiegeln diese Entwicklung wider.

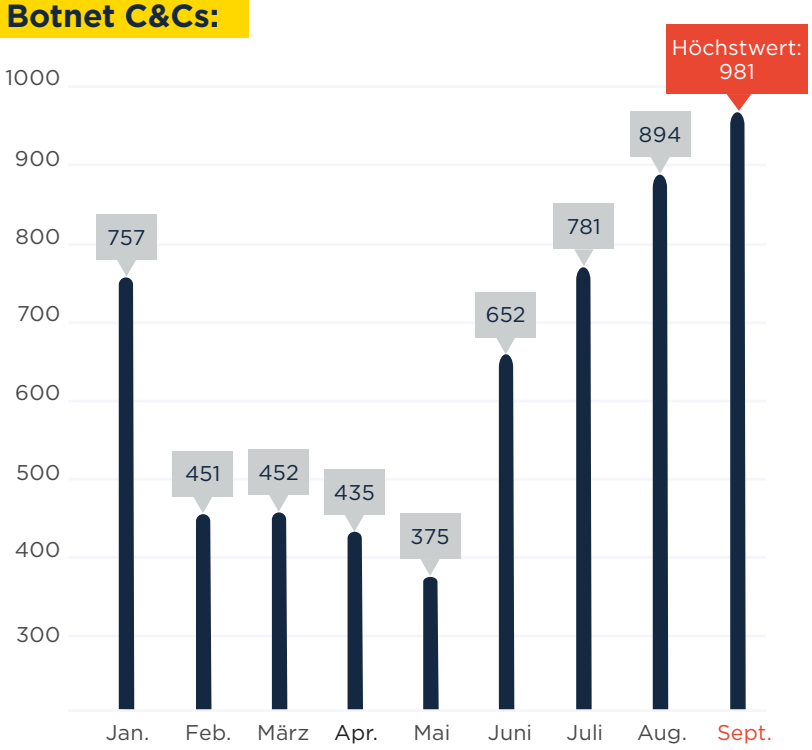
Was ist FluBot?

FluBot ist ein Trojaner, der Android-Geräte infiziert. Er stiehlt Anmeldedaten von Nutzern und breitet sich aus, indem er das infizierte Smartphone in einen Zombie verwandelt, der SMS-Spam verbreitet.

Anzahl der erkannten Botnet C&Cs, Q3-2021

Die Spamhaus Malware Labs konnten im 3. Quartal 2021 insgesamt 2.656 Botnet C&Cs identifizieren, im Vergleich zu 1.462 im 2. Quartal 2021. Das bedeutet einen Anstieg um sage und schreibe 82 % innerhalb eines Quartals! Der Monatsdurchschnitt stieg von 487 in Q2 auf 885 Botnet C&Cs in Q3.

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



Quartal	Anzahl von Botnets	Quartalsdurchschnitt	% Veränderung
Q1	1660	553	24 %
Q2	1462	487	-12 %
Q3	2656	885	82 %

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, Q3-2021

Angesichts des Einflusses von FastFlux im vergangenen Quartal überrascht es nicht weiter, dass ein klares Muster zu erkennen ist, nach dem die Neuzugänge in die Top 20 in Q3 strömen. Viele der Länder, die neu in der Rangordnung sind, waren für einen hohen Prozentsatz der Botnet-C&C-Server TeamBot und FluBot verantwortlich, die FastFlux nutzen, und entsprechen dem Profil von Ländern mit hoher Internetverbreitung aber eher geringem Sicherheitsbewusstsein.

Neuzugänge

Mexiko (Nr. 4), Saudi-Arabien (Nr. 7), Dominikanische Republik (Nr. 8), Korea (Nr. 10), Uruguay (Nr. 11), Argentinien (Nr. 14), Schweden (Nr. 18), Rumänien (Nr. 20).

Abgänge

Ukraine, Seychellen, Panama, Kanada, Malaysia, Polen, Finnland, Türkei.

Beträchtliche Zunahmen in Russland

Die Anzahl der in Russland ansässigen Botnet C&Cs hat drastisch zugenommen. Dies ist bereits das zweite Quartal in Folge, in dem Russland einen starken Zuwachs verzeichnet:

- Q1 bis Q2 – Zunahme um 19 %
- Q2 bis Q3 – Zunahme um 64 %

Daher ist es wenig überraschend, dass Russland im 3. Quartal die USA von Platz 1 verdrängt hat.

Kontinuierlicher Anstieg in Europa

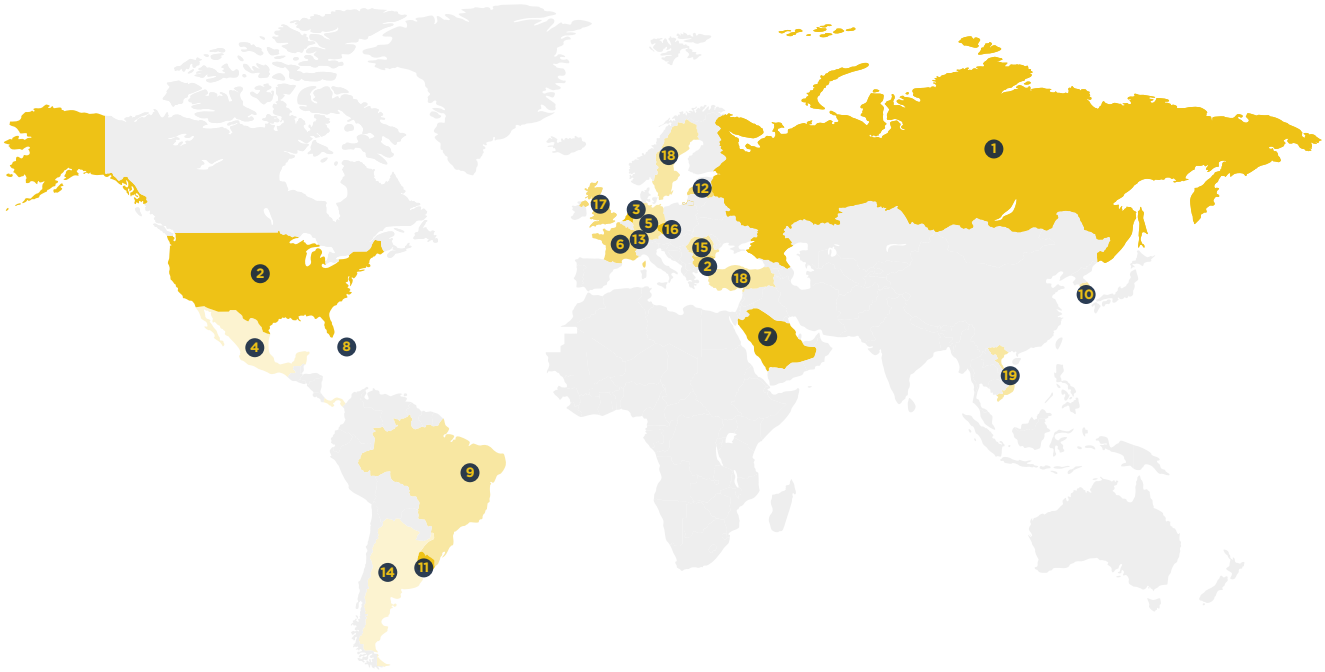
Der Trend, der schon im 2. Quartal zu beobachten war, setzt sich im 3. Quartal fort. Wieder war eine Zunahme der Zahl der Botnet C&C-Server in verschiedenen europäischen Ländern zu verzeichnen, unter anderem in den Niederlanden (+63 %), Deutschland (+45 %), Frankreich (+34 %) und der Schweiz (+34 %).

Geografische Verteilung der Botnet C&Cs, Q3-2021 (Fortsetzung)

Top 20 Botnet C&C-Hosting-Länder

Rang	Land	Q2-2021	Q3-2021	% Veränderung gegenüber dem vorigen Quartal
1.	Russland	233	381	64 %
2.	USA	281	301	7 %
3.	Niederlande	168	273	63 %
4.	Mexiko	-	182	Neuzugang
5.	Deutschland	117	170	45 %
6.	Frankreich	92	123	34 %
7.	Saudi-Arabien	-	117	Neuzugang
8.	Dominikanische Republik	-	96	Neuzugang
9.	Brasilien	12	86	617 %
10.	Korea	-	68	Neuzugang

Rang	Land	Q2-2021	Q3-2021	% Veränderung gegenüber dem vorigen Quartal
11.	Uruguay	-	63	Neuzugang
12.	Lettland	84	58	-31 %
13.	Schweiz	41	55	34 %
14.	Argentinien	-	50	Neuzugang
15.	Moldawien	29	49	69 %
16.	Tschechische Republik	31	40	29 %
17.	Großbritannien	57	39	-32 %
18.	Schweden	-	38	Neuzugang
19.	Vietnam	13	34	162 %
20.	Rumänien	-	33	Neuzugang



Mit Botnet C&Cs assoziierte Malware, Q3-2021

Hier sind die Spitzenreiter aus der Szene der Malware-Familien, die mit den neu beobachteten Botnet C&Cs im 3. Quartal 2021 assoziiert werden.

TeamBot und FluBot im Aufwind

Ist Ihnen TeamBot ein Begriff? Vermutlich nicht. Auch wenn es sich weder um eine neue noch um eine ernsthafte Bedrohung handelt, führt TeamBot die Hitliste zusammen mit FluBot an, beides Backdoors.

Unsere Threat Hunter sind der Ansicht, dass TeamBot und FluBot dieselbe FastFlux-Infrastruktur nutzen und dieselben Botnet C&C-IP-Adressen alle paar Minuten rotieren – daher der gemeinsame Rang in der Liste.

In diesem Quartal gab es eine explosionsartige Zunahme bei Backdoor Malware, die sich damit im 3. Quartal 2021 zum vorrangigen, mit Botnet C&C assoziierten Malware-Typ entwickelt hat.

RedLine gewinnt, Raccoon verliert

2021 beobachten wir einen Kampf um die Poleposition zwischen RedLine und Raccoon, beides Credential Stealer, die im Darknet käuflich zu erwerben sind. Während im 2. Quartal 2021 mit 571 % ein gewaltiger Anstieg von Botnet C&C-Servern von Raccoon zu verzeichnen war, erlebte die Malware RedLine im 3. Quartal 2021 einen Zuwachs von 71 % und verdrängte damit Raccoon von der Spitzenposition.

IcedID verschwindet

IcedID ist in diesem Jahr relativ inaktiv und trat im 2. Quartal nur kurz auf Platz 18 in Erscheinung, um dieses Quartal wieder zu verschwinden. Der Grund dafür ist nicht bekannt. Unser Rechercheteam geht jedoch davon aus, dass die Ruhe trügerisch ist und nicht lange anhalten wird. IcedID ist einer der Trojaner, die von Ransomware-Gruppen im Darknet käuflich erworben werden können. Über diese Trojaner wird der Zugang zu Unternehmensnetzwerken verkauft, ein überaus lukratives Geschäft.

Was ist Backdoor Malware?

Diese Art von Malware umgeht die üblichen Authentifizierungsverfahren und andere Sicherheitsvorkehrungen, um sich auf hoher Ebene Zugang zu einem System, einem Netzwerk oder einer Anwendung zu verschaffen.

Neuzugänge

TeamBot (Nr. 1), FluBot (Nr. 1), Smoke Loader (Nr. 9), AveMaria (Nr. 13).

Abgänge

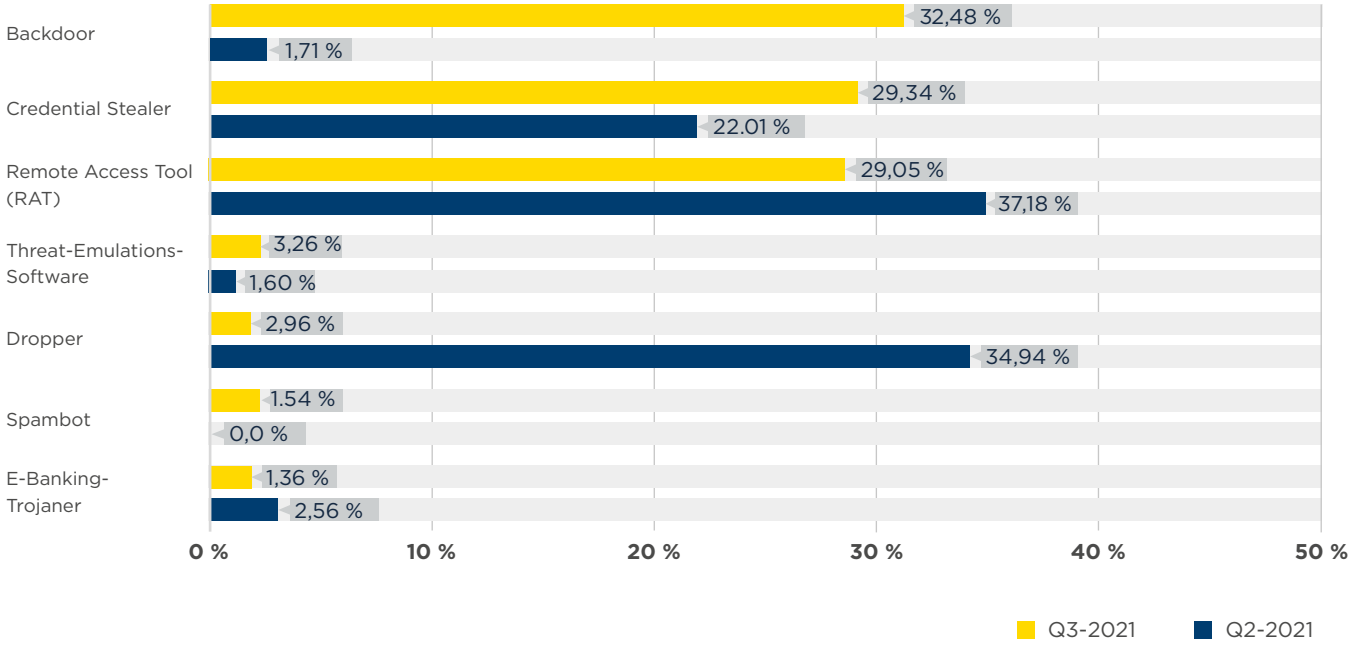
Oski, IcedID, Arkei.

Mit Botnet C&Cs assoziierte Malware, Q3-2021 (Fortsetzung)

Mit Botnet C&Cs assoziierte Malware-Familien

Rang	Q2-2021	Q3-2021	% Veränderung	Malware-Familie	Beschreibung
1.	-	507	Neuzugang	TeamBot & FluBot	Backdoor
2.	123	210	71 %	RedLine	Credential Stealer
3.	42	136	224 %	BitRAT	Remote Access Tool (RAT)
4.	83	121	46 %	AsyncRAT	Remote Access Tool (RAT)
5.	66	108	64 %	Loki	Credential Stealer
6.	302	93	-69 %	Raccoon	Credential Stealer
7.	24	71	196 %	NjRAT	Remote Access Tool (RAT)
8.	15	55	267 %	Cobalt Strike	Backdoor
9.	-	50	Neuzugang	Smoke Loader	Dropper
10.	26	43	65°%	Vjw0rm	Credential Stealer
11.	16	41	156 %	CryptBot	Backdoor
12.	24	40	67 %	RemcosRAT	Remote Access Tool (RAT)
13.	-	37	Neuzugang	AveMaira	Remote Access Tool (RAT)
13.	23	37	61 %	NanoCore	Remote Access Tool (RAT)
15.	17	30	76 %	STRRAT	Remote Access Tool (RAT)
16.	23	26	13 %	Tofsee	Spambot
17.	14	24	71 %	ServHelper	Credential Stealer
18.	43	23	-47 %	Gozi	E-Banking-Trojaner
19.	11	18	64 %	QuasarRAT	Remote Access Tool (RAT)
20.	23	17	-26 %	AgentTesla	Credential Stealer

Vergleich der Malware-Typen zwischen Q2- und Q3-2021



Die am häufigsten missbrauchten Top Level Domains, Q3-2021

Keine Veränderung an der Spitze

Auch im 3. Quartal nehmen .com und .xyz die Spitzenplätze unserer Rangliste ein. Für diese beiden TLDs hat sich die Situation verschlechtert, speziell für .com mit einem Zuwachs von 90 %. Wir hoffen, dass VeriSign und XYZ.COM, die Inhaber dieser TLDs, alle Maßnahmen ergreifen werden, die notwendig sind, um die Lage in den Griff zu bekommen und die Reputation ihrer TLDs zu verbessern.

Drei neue TLDs

Es gibt zwei neue gTLDs und eine ccTLD in den Top 20: .club, .co und .monster. Alle verzeichnen einen kräftigen Anstieg der Anzahl neuer Botnet C&C-Domains, die über ihren Dienst registriert werden.

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.

Neuzugänge

club (Nr. 9), co (Nr. 18), monster (Nr. 19).

Abgänge

vip, online, live.

Die am häufigsten missbrauchten Top Level Domains, Q3-2021 (Fortsetzung)

Die am häufigsten missbrauchten TLDs – Anzahl der Domains

Rang	Q2-2021	Q3-2021	% Veränderung	TLD	Typ
1.	4113	7827	90 %	com	gTLD
2.	739	833	13 %	xyz	gTLD
3.	607	829	37 %	top	gTLD
4.	146	665	355 %	net	gTLD
5.	662	538	-19 %	buzz	ccTLD
6.	151	330	119 %	ru	ccTLD
7.	139	306	120 %	cn	ccTLD
8.	157	265	69 %	org	gTLD
9.	140	183	31 %	tk	Ursprünglich ccTLD, jetzt effektiv gTLD
9.	80	183	129 %	su	ccTLD
9.	-	183	Neuzugang	club	gTLD
12.	78	178	128 %	info	gTLD
13.	208	170	-18 %	br	ccTLD
14.	106	132	25 %	ga	Ursprünglich ccTLD, jetzt effektiv gTLD
15.	116	126	9 %	eu	ccTLD
16.	104	123	18 %	ml	Ursprünglich ccTLD, jetzt effektiv gTLD
17.	73	98	34 %	cf	ccTLD
18.	-	89	Neuzugang	co	ccTLD
19.	-	82	Neuzugang	monster	gTLD
19.	141	82	-42 %	cloud	gTLD

Am häufigsten missbrauchte Domain-Registrierungsstellen, Q3-2021

Bei den meisten in unseren Top 20 geführten Domain-Registrierungsstellen konnten wir beträchtliche Zunahmen beobachten. Der höchste Prozentsatz der Domain-Registrierungsstellen ist in China ansässig, gefolgt von Kanada und den USA. Während die prozentualen Anteile von Kanada und Indien gesunken sind, haben viele der gelisteten Unternehmen in diesem Jahr zugelegt*.

Arsys nicht mehr in der Rangliste

Arsys lag im 2. Quartal noch als Neuzugang auf Rang 5. Dort hat man anscheinend sachdienliche Maßnahmen ergriffen, um die TLD so sauber wie möglich zu halten, und ist konsequenterweise im 3. Quartal nicht mehr in den Top 20 vertreten. Gleiches gilt für HiChina, 1API, Name.com und 55hl.com. Glückwunsch an diese Registrierungsstellen.

Probleme mit Resellern

Im 3. Quartal war die größte Zunahme bei neu registrierten Botnet C&C Domains bei CentralNic (+488 %), Tucows (+266 %), RegRU (+252 %), West263.com (+168 %) und Network Solutions (+163 %) zu verzeichnen.

Die große Mehrzahl der betrügerischen Registrierungen von Domain Names stammen von armen Resellern, die ihre Kunden nicht hinlänglich überprüfen – wenn überhaupt.

Es fällt den Registrierungsstellen aus verschiedenen Grünen schwer, diese „schmutzigen“ Reseller zu sanktionieren, unter anderem aufgrund schlecht formulierter Nutzungsbedingungen. Doch auch andere Elemente spielen eine Rolle, wie beispielsweise finanzielle Interessen oder die mangelnde Motivation, die Verantwortung für diese Probleme zu übernehmen.

Wir hoffen, dass diese Registrierungsstellen gelingen wird, ihre Reputation zu verbessern, indem sie ihre Reseller möglichst umgehend dazu zwingen, sich im Kampf gegen die Registrierung betrügerischer Domain Names stärker zu bemühen.

Registrierungsstellen und Botnet C&C-Betreiber

Cyberkriminelle müssen eine Registrierungsstelle finden, um sich 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

Porkbun (Nr. 7), dnspod.cn (Nr. 11), nicenic.net (Nr. 13), Openprovider (Nr. 18), OVH (Nr. 19).

Abgänge

Arsys, HiChina, Name.com, 55hl.com, 1API.

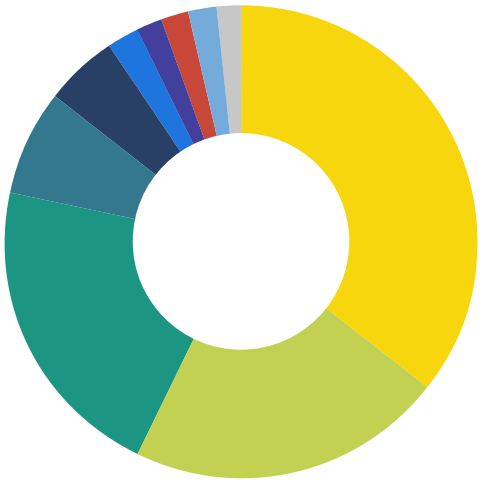
* Aktualisiert am 15. Oktober 2021 | Zwei Registrierungsstellen (NameSilo und Tucows) waren zum Zeitpunkt der ursprünglichen Veröffentlichung dieses Berichts als US-amerikanische Anbieter aufgeführt. Wir haben den Text und die Daten aktualisiert, um widerzuspiegeln, dass sie in Kanada ansässig sind.

Am häufigsten missbrauchte Domain-Registrierungsstellen, Q3-2021 (Fortsetzung)

Am häufigsten missbrauchte Domain-Registrierungsstellen – Anzahl der Domains

Rang	Q2-2021	Q3-2021	% Veränderung	Registrierungsstelle	Land
1.	1797	1568	–13 %	NameSilo	Kanada*
2.	955	1267	33 %	Namecheap	USA
3.	504	1217	141 %	Alibaba	China
4.	526	787	50 %	eName Technology	China
5.	112	658	488 %	CentralNic	Großbritannien
6.	135	475	252 %	RegRU	Russland
7.	110	403	266 %	Tucows	Kanada*
7.	-	403	Neuzugang	Porkbun	USA
9.	101	266	163 %	Network Solutions	USA
10.	125	255	104 %	Xin Net	China
11.	80	214	168 %	west263.com	China
11.	-	214	Neuzugang	dnspod.cn	China
13.	-	209	Neuzugang	nicenic.net	China
14.	215	189	–12 %	Eranet International	China
15.	92	188	104 %	Key Systems	Deutschland
16.	110	176	60 %	22net	China
17.	188	169	–10 %	PDR	Indien
18.	-	165	Neuzugang	Openprovider	Niederlande
19.	-	160	Neuzugang	OVH	Frankreich
20.	91	154	69 %	WebNic.cc	Singapur

Standort der am häufigsten missbrauchten Domain-Registrierungsstellen



Land	Botnets	%
China	3261	35,7 %
Kanada*	1971	21,57 %
USA	1936	21,19 %
Großbritannien	658	7,2 %
Russland	475	5,2 %
Deutschland	188	2,1 %
Indien	169	1,8 %
Niederlande	165	1,8 %
Frankreich	160	1,8 %
Singapur	154	1,7 %
Gesamt	**9137**	

* Aktualisiert am 15. Oktober 2021 | Zwei Registrierungsstellen (NameSilo und Tucows) waren zum Zeitpunkt der ursprünglichen Veröffentlichung dieses Berichts als US-amerikanische Anbieter aufgeführt. Wir haben den Text und die Daten aktualisiert, um widerzuspiegeln, dass sie in Kanada ansässig sind.

Netzwerke, welche die meisten neu erkannten Botnet C&Cs hosten, Q3-2021

Wie üblich gab es eine ganze Reihe von Veränderungen bei den Netzwerken, die neu erkannte Botnet C&Cs hosten. Insbesondere gab es einen Zustrom von Netzwerken, die FastFlux Botnet C&Cs hosten. Diese werden von Cyberkriminellen als Host für Backdoor Malware missbraucht.

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“.

serverion.com

Wir konnten eine Zunahme von 69 % bei der Anzahl neuer Botnet C&C-Server beim niederländischen Hosting-Provider serverion.com beobachten. Unsere Experten sind der Ansicht, dass dieser Anstieg in erster Linie auf den Downstream-Kunden des.capital zurückzuführen ist, der für Botnet-Betreiber überaus attraktiv zu sein scheint.

Positive Veränderungen

In unserem vorigen Quartalsbericht konnten wir den Umzug eines Botnet-Hosting-Betreibers von Amazon zu DigitalOcean vermelden, der dem Letztgenannten zur zweifelhaften Ehre eines Rangs in unseren Top 20 verhalfen. Nun beglückwünschen wir DigitalOcean dazu, im 3. Quartal 2021 wieder aus unserer Top-20-Rangliste verschwunden zu sein, ebenso wie Google, die an Nr. 2 standen, HostSailor, Microsoft, M247 und Off Shore Racks.

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 in Kraft zu haben, 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

uninet.net.mx (Nr. 1), stc.com.sa (Nr. 3), claro.com.do (Nr. 4), antel.net.uy (Nr. 8), telefonica.com.br (Nr. 9), telefonica.com.ar (Nr. 16), uplus.co.kr (Nr. 17), hotwinds.com (Nr. 18).

Abgänge

google.com, itld.com, digitalocean.com, internet-it, hostsailor.com, microsoft.com, m247.ro, offshoreracks.com.

Netzwerke, welche die meisten neu erkannten Botnet C&Cs hosten, Q3-2021 (Fortsetzung)

Neu erkannte Botnet C&Cs pro Netzwerk

Rang	Q2-2021	Q3-2021	% Veränderung	Netzwerk	Land
1.	-	177	Neuzugang	uninet.net.mx	Mexiko
2.	68	115	69 %	serverion.com	Niederlande
3.	-	105	Neuzugang	stc.com.sa	Saudi-Arabien
4.	-	95	Neuzugang	claro.com.do	Dominikanische Republik
5.	48	89	85 %	privacyfirst.sh	Deutschland
6.	35	69	97 %	ipjetable.net	Frankreich
7.	29	68	134 %	cloudflare.com	USA
8.	-	63	Neuzugang	antel.net.uy	Uruguay
9.	-	58	Neuzugang	telefonica.com.br	Brasilien
10.	82	56	-32 %	pq.hosting	Russland
11.	56	52	-7 %	ovh.com	Frankreich
12.	46	51	11 %	hetzner.de	Deutschland
13.	16	45	181 %	mivocloud.com	Moldawien
14.	40	44	10 %	baxet.ru	Russland
14.	49	44	-10 %	nano.lv	Lettland
16.	-	43	Neuzugang	telefonica.com.ar	Argentinien
17.	-	41	Neuzugang	uplus.co.kr	Korea
18.	26	33	27 %	alibaba-inc.com	China
18.	-	33	Neuzugang	hotwinds.com	USA
20.	47	32	-32 %	mgnhost.ru	Russland

Netzwerke, welche die aktivsten Botnet C&Cs hosten, Q3-2021

Zum guten Schluss sehen wir uns die Netzwerke an, die im 3. 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.

Eine Zunahme beim Botnet C&C-Missbrauch

Leider hat sich die Situation in Bezug auf aktive Botnet-C&C-Missbrauch für viele ISPs, die im 2. Quartal schon in unserer Top-20-Liste waren, weiter verschlechtert. Ipjetable.net (FR), microsoft.com (US), vietserver.vn (VN) und openvpn (SE) haben eines gemeinsam: Anstatt angemessene Maßnahmen gegen den Missbrauch ihrer Infrastruktur zu treffen, ist die Zahl der aktiven Botnet C&C-Server in diesen Netzwerken weiter gestiegen.

uninet.net.mx und stc.com.sa

Diese beiden ISPs sind aufgrund der großen Zahl von FastFlux-Bots, die in ihren Netzwerken gehostet werden, dieses Quartal an Nr. 1 und Nr. 2 unserer Top 20 aufgestiegen.

Tatsächlich ist der Großteil der Neuzugänge auf das Hosten von FastFlux-Bots in den betreffenden Netzwerken und die zögerliche Reaktion auf Missbrauchsmeldungen zurückzuführen. Alle diese Unternehmen bieten einen nachhaltigen Nährboden für Botnet-Betreiber.

Neuzugänge

uninet.net.mx (Nr. 1), stc.com.sa (Nr. 2), claro.com.do (Nr. 4), antel.net.uy (Nr. 6), telefonica.com.br (Nr. 7), telefonica.com.ar (Nr. 8), tie.cl (Nr. 10), serverion.com (Nr. 10), algartelecom.com.br (Nr. 14), uplus.co.kr (Nr. 17), skbroadband.com (Nr. 19).

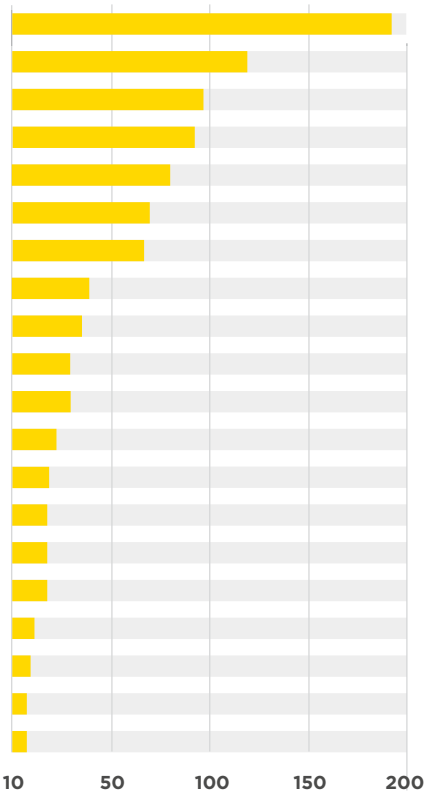
Abgänge

google.com, ttnet.com.tr, inmotionhosting.com, m247.ro, datawire.ch, mtnnigeria.net, eliteteam.to, unusinc.com, chinanet-js, kornet.net.

Netzwerke, welche die aktivsten Botnet C&Cs hosten, Q3-2021 (Fortsetzung)

Gesamtzahl aktiver Botnet C&Cs pro Netzwerk

Rang	Q2-2021	Q3-2021	% Veränderung	Netzwerk	Land
1.	-	185	Neuzugang	uninet.net.mx	Mexiko
2.	-	119	Neuzugang	stc.com.sa	Saudi-Arabien
3.	61	99	62 %	ipjetable.net	Frankreich
4.	-	97	Neuzugang	claro.com.do	Dominikanische Republik
5.	58	79	36 %	microsoft.com	USA
6.	-	68	Neuzugang	antel.net.uy	Uruguay
7.	-	63	Neuzugang	telefonica.com.br	Brasilien
8.	-	41	Neuzugang	telefonica.com.ar	Argentinien
9.	23	32	39 %	vietserver.vn	Vietnam
10.	-	29	Neuzugang	tie.cl	Chile
10.	-	29	Neuzugang	serverion.com	Niederlande
12.	20	24	20 %	ovpn.com	Schweden
13.	21	22	5 %	charter.com	USA
14.	-	21	Neuzugang	algartelecom.com.br	Brasilien
14.	18	21	17 %	cloudvider.net	Großbritannien
14.	17	21	24 %	une.net.co	Kolumbien
17.	-	19	Neuzugang	uplus.co.kr	Korea
18.	17	18	6 %	hostry.com	Zypern
19.	-	17	Neuzugang	skbroadband.com	Korea
19.	12	17	42 %	claro.com.co	Kolumbien



Damit verabschieden wir uns für heute.

Im Januar sehen wir uns wieder. Bleiben Sie gesund!