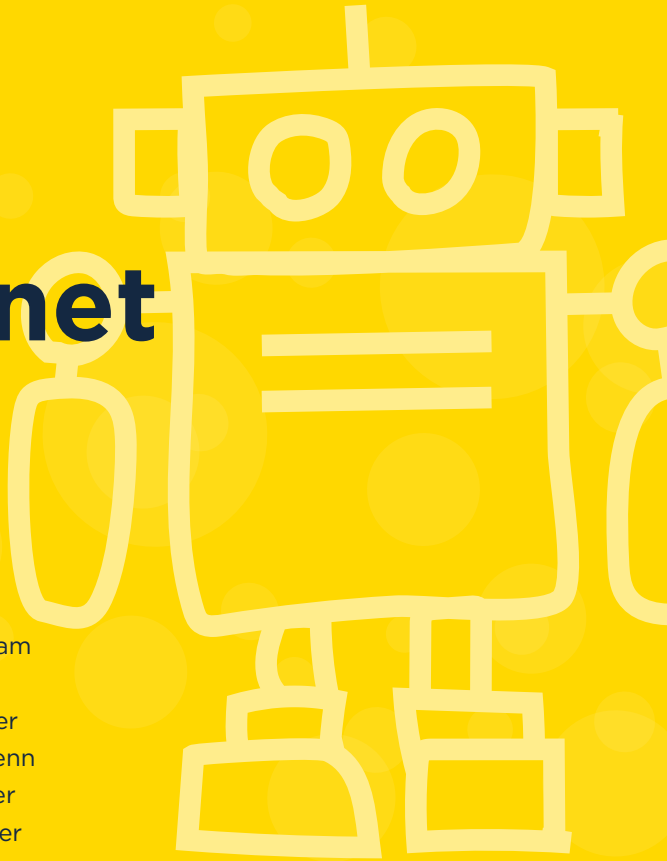
SPAMHAUS



Spamhaus Botnet Threat Update

Q4-2021

Im 4. Quartal stieg die Zahl der neuen von unserem Rechercheteam identifizierten Botnet-Command-and-Control-Aktivitäten (C&Cs) um 23 %. Dabei ist unseren Experten bewusst, dass sie trotz dieser Zunahme nicht alle Botnet-C&C-Aktivitäten verfolgen können, wenn deren Kommunikation über DNS over HTTPS (DoH) erfolgt. Dieser Umstand gibt Anlass zur Sorge und lässt die Waage zugunsten der Cyberkriminellen kippen.

Willkommen beim Spamhaus Botnet Threat Update für das 4. 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 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

Die Probleme mit DNS over HTTPS (DoH)

Erinnern Sie sich noch an FluBot und TeamBot aus dem 3. Quartal?

Im vergangenen Quartal berichteten wir über „eine explosionsartige Zunahme von Backdoor-Malware“ aufgrund von FluBot und TeamBot. Im 4. Quartal ist diese Malware-Familie aus Sicht der von Spamhaus beobachteten Botnet-C&C-Infrastruktur vollständig verschwunden. Das heißt jedoch nicht, dass sie aufgehört hat aktiv zu sein. Ganz im Gegenteil, sie ist sogar sehr aktiv!

Warum wird sie dann nicht von Spamhaus erkannt?

Diese Malware erscheint nicht in unseren Listen, weil ihre Urheber ihre Vorgehensweise geändert haben. Anstatt die C&C-Kommunikation über das traditionelle HTTPS-Protokoll laufen zu lassen, verwenden sie DNS over HTTPS (DoH) und missbrauchen große DoH-Anbieter wie Google und Alibaba.

Die Vermeidung von Missbrauch im Internet wird schwieriger

Als DoH von der Allgemeinheit noch mit großem Hallo begrüßt und als beste neue Sicherheitsentwicklung gefeiert wurde, erkannten manche Sicherheitsprofis (wie auch Spamhaus) bereits, dass die Betrügereien der Kriminellen damit noch schwerer aufzudecken sein würden. Und mit „noch schwerer aufzudecken“ beziehen wir uns auf andere Probleme wie die abnehmende Transparenz der WHOIS-Daten.[1]

(1) www.spamhaus.org/news/article/775/how-has-gdpr-affected-spam

Warum ist DoH so problematisch?

DoH verschlüsselt den DNS-Datenverkehr und macht eine Ressource, die bisher öffentlich (d. h. unverschlüsselt) war, privat und sicher. Das klingt doch erstmal gut, könnte man meinen. Allerdings führt es dazu, dass unsere Recherchespezialisten keinen Einblick in die DNS-Abfragen von FluBot und TeamBot haben. Daher können wir die IP-Adressen nicht in unseren Listen führen, und somit stehen diese Daten auch nicht für den Schutz der Nutzer zur Verfügung. Obwohl DoH eigentlich die Internetgemeinde schützen soll, profitieren davon auch die Cyberkriminellen. Ein zweischneidiges Schwert.

DoH erschwert nicht nur die Jagd nach Betrügern. Es bedeutet auch, dass Sicherheitsprodukte rund um die DNS-Überwachung und -Filterung möglicherweise weniger wirksam sind, was nicht wünschenswert ist. Sicherheitsprobleme werden verschärft, wenn große DoH-Anbieter schädliche DNS-Auflösungen von Botnet-, Phishing- oder Malware-Domains nicht herausfiltern.

Anzahl der erkannten Botnet C&Cs, Q4-2021

Im 4. Quartal 2021 identifizierte Spamhaus 3.271 Botnet C&Cs gegenüber 2.656 im 3. Quartal 2021. Das bedeutet einen Anstieg um 23 % innerhalb eines Quartals. Der Monatsdurchschnitt stieg von 885 im 3. Quartal auf 1090 Botnet C&Cs im 4. Quartal.

Quartal	Anzahl von Botnets	Quartalsdurchschnitt	% Veränderung
Q1	1660	553	24 %
Q2	1462	487	-12 %
Q3	2656	885	82 %
Q4	3271	1090	23 %

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, Q4-2021

Weiterhin beträchtliche Zunahmen in Russland

Im vergangenen Quartal berichteten wir von einer starken Zunahme der Zahl der Botnet C&Cs in Russland. In diesem Quartal war die Steigerung allerdings noch größer:

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

Im 4. Quartal befanden sich knapp 30 % aller Botnet C&C Server in Russland.

Neuzugänge

Ukraine (Platz 12), Bulgarien (15), Seychellen (17), Hongkong (18).

Abgänge

Korea, Schweiz, Argentinien, Vietnam.

Lateinamerika weiterhin präsent

Im 3. Quartal waren mehrere Neuzugänge aus Lateinamerika (LatAm) zu verzeichnen, die auch im 4. Quartal wieder in den Top 20 vertreten sind, darunter Mexiko, die Dominikanische Republik, Brasilien und Uruguay. Uruguay wies dabei mit 181 % den größten prozentualen Anstieg aller Geografien im 4. Quartal auf.

Auf und ab in Europa

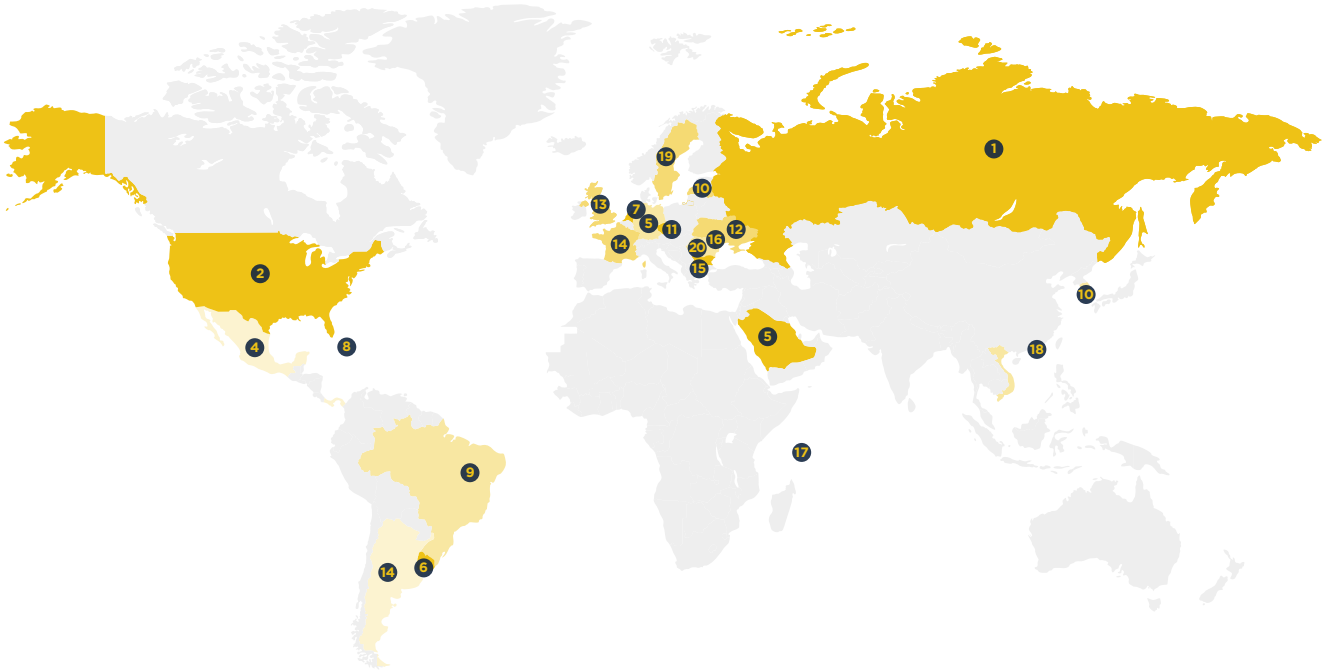
Nach dem kontinuierlichen Anstieg in einigen europäischen Ländern freut es uns, nun Abnahmen beispielsweise in den Niederlanden, Frankreich, Schweden und Rumänien melden zu können. Die Schweiz ist zwischenzeitlich sogar ganz aus den Top 20 verschwunden. Allerdings findet sich Deutschland mit einem Plus von 35 % auf dem 3. Rang wieder, während in Großbritannien eine Zunahme von 56 % zu beobachten war.

Geografische Verteilung der Botnet C&Cs, Q4-2021 (Fortsetzung)

Top 20 Botnet C&C-Hosting-Länder

Rang	Land	Q3-2021	Q4-2021	% Veränderung gegenüber dem vorigen Quartal
1.	Russland	381	854	124 %
2.	USA	301	384	28 %
3.	Deutschland	170	230	35 %
4.	Mexiko	182	186	2 %
5.	Saudi-Arabien	117	180	54 %
6.	Uruguay	63	177	181 %
7.	Niederlande	273	164	-40 %
8.	Dominikanische Republik	96	110	15 %
9.	Brasilien	86	92	7 %
10.	Lettland	58	69	19 %

Rang	Land	Q3-2021	Q4-2021	% Veränderung gegenüber dem vorigen Quartal
11.	Tschechische Republik	40	66	65°%
12.	Ukraine	-	64	Neuzugang
13.	Großbritannien	39	61	56 %
14.	Frankreich	123	60	-51 %
15.	Bulgarien	-	56	Neuzugang
16.	Moldawien	49	50	2 %
17.	Seychellen	-	34	Neuzugang
18.	Hongkong	-	28	Neuzugang
19.	Schweden	38	26	-32 %
20.	Rumänien	33	24	-27 %



Mit Botnet C&Cs assoziierte Malware, Q4-2021

Credential Stealers waren im 4. Quartal der am stärksten verbreitete Malware-Typ im Zusammenhang mit Botnet C&Cs. Das ist nicht weiter überraschend angesichts der Tatsache, dass die beiden Malware-Spitzenreiter unserer Listen, RedLine und Loki, beides Credential Stealers sind.

GCleaner legt zu

Beträchtlichen Aufwind sahen wir bei GCleaner, der als Newcomer direkt auf Rang 4 in die Top 20 eingestiegen ist. Die Vorgehensweise von GCleaner ist mit der von Smoke Loader vergleichbar: ein Pay-Per-Install-Modell (PPI), das auf bereits infizierten Hosts weitere Malware ablegt. Auch wenn diese Malware-Bedrohung bereits einige Zeit herumspukt, hat es GCleaner nun erstmalig in unsere Top 20 geschafft.

FluBot/TeamBot verschwinden

Wie im Abschnitt „Im Blickpunkt“ besprochen, ist diese Malware, die im vergangenen Quartal noch auf Platz 1 unserer Rangliste stand, jetzt völlig daraus verschwunden. Allerdings treibt sie weiter ihr Unwesen, mittlerweile jedoch über DoH.

Neuzugänge

GCleaner (Platz 4), DCRat (10), Arkei (14), TrickBot (15), Socelars (16).

Abgänge

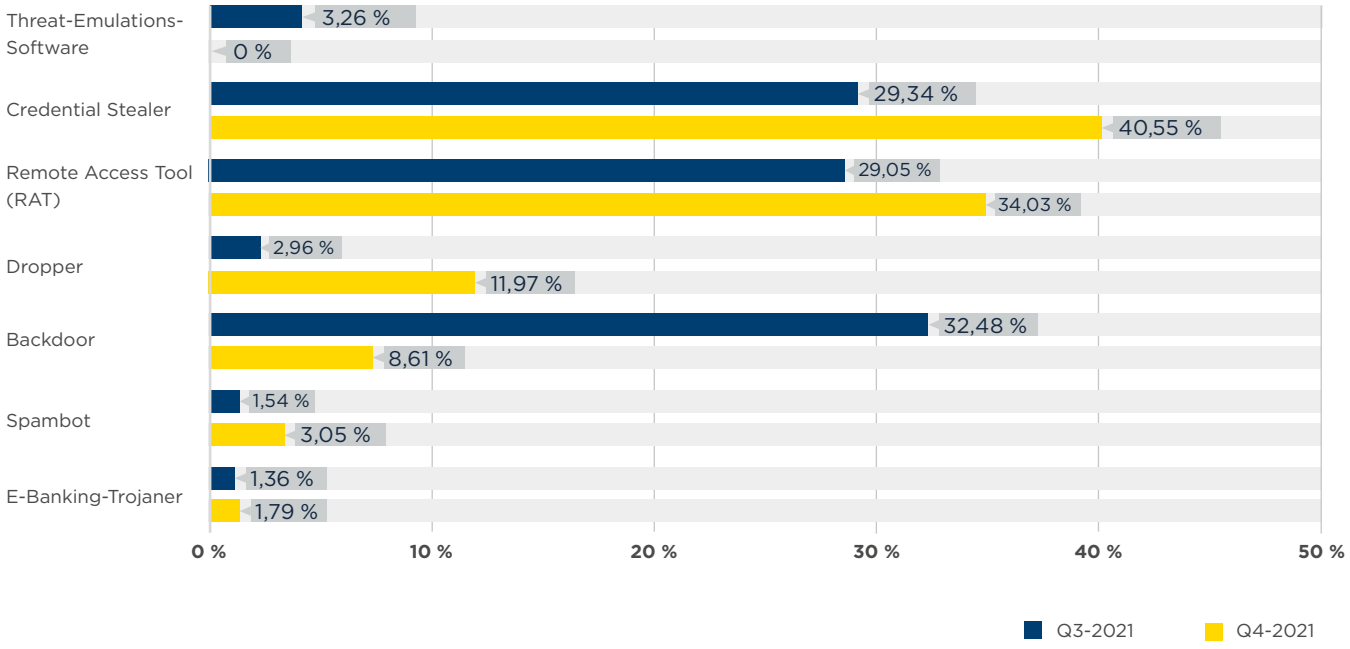
FluBot/TeamBot, AveMaria, ServHelper, QuasarRAT, AgentTesla.

Mit Botnet C&Cs assoziierte Malware, Q4-2021 (Fortsetzung)

Mit Botnet C&Cs assoziierte Malware-Familien

Rang	Q3-2021	Q4-2021	% Veränderung	Malware-Familie	Beschreibung
1.	210	164	-22 %	RedLine	Credential Stealer
2.	108	102	-6 %	Loki	Credential Stealer
3.	121	91	-25 %	AsyncRAT	Remote Access Tool (RAT)
4.	-	86	Neuzugang	GCleaner	Dropper
5.	93	75	-19 %	Raccoon	Credential Stealer
6.	43	65	51 %	Vjw0rm	Remote Access Tool (RAT)
7.	41	43	5 %	CryptBot	Backdoor
8.	136	37	-73 %	BitRAT	Remote Access Tool (RAT)
9.	71	36	-49 %	NjRAT	Remote Access Tool (RAT)
10.	-	32	Neuzugang	DCRat	Remote Access Tool (RAT)
11.	26	29	12 %	Tofsee	Spambot
11.	40	29	-28 %	Remocs	Remote Access Tool (RAT)
13.	50	28	-44 %	Smoke Loader	Dropper
14.	-	27	Neuzugang	Arkei	Credential Stealer
15.	-	21	Neuzugang	TrickBot	Backdoor
16.	-	18	Neuzugang	Socelars	Credential Stealer
16.	55	18	-67 %	CobaltStrike	Backdoor
18.	23	17	-26 %	Gozi	E-Banking-Trojaner
18.	37	17	-54 %	NanoCore	Remote Access Tool (RAT)
18.	30	17	-43 %	STRRAT	Remote Access Tool (RAT)

Vergleich der Malware-Typen zwischen Q4- und Q3-2021



Die am häufigsten missbrauchten Top Level Domains, Q4-2021

Neuzugang an Nr. 4

Wir erleben nicht allzu häufig TLD-Neuzugänge auf den ersten fünf Rängen dieser Botnet C&C Top 20, nun allerdings .xxx, eine von der Registrierungsstelle ICM betriebene TLD für Erwachsene als Neueinstieg auf Nr. 4. Angesichts der weniger als 10.000 aktiven Domains aber insgesamt 223 Domains, die im 4. Quartal mit Botnet-C&C-Aktivitäten assoziiert wurden, müssen wir davon ausgehen, dass es dort Probleme gibt.

.de ist wieder da

Nachdem die ccTLD .de (Deutschland) im 2. Quartal zunächst aus den Top 20 verschwunden war, ist sie nun auf Platz 20 wieder eingestiegen.

Abnahmen und Abgänge

Herzlichen Glückwunsch an alle Registrierungsstellen von TLDs, die nicht mehr in unseren Listen auftauchen, und allen, denen es gelungen ist, die Zahl der mit ihren TLDs assoziierten Botnet C&Cs deutlich zu verringern. Dazu gehören beispielsweise .buzz und .net, die jeweils einen Rückgang von 80 % verzeichnen konnten.

Ein Fehler in den Q3-Daten

Wir bitten Verisign für eine fehlerhafte Angabe in unserer Statistik von Q3-2021 für .com um Entschuldigung. Die richtige Zahl der Botnet C&Cs für die TLD lautet 3.730. Dieser Fehler hatte mehrere Gründe, doch wir freuen uns, dass wir ihn nun in Zusammenarbeit mit Verisign berichtigen konnten.

Auslegung der Daten

Registrierungsstellen mit einer höheren Anzahl aktiver Domains sind per se anfälliger für Missbrauch. Beispielsweise hatte .net im 4. Quartal 2021 über 13 Millionen aktive Domain-Zonen, von denen 0,00103 % mit Botnet C&Cs in Verbindung gebracht wurden. Hingegen hatte .xxx gut 9.000 aktive Domains, von denen 2,4 % mit Botnet C&Cs assoziiert wurden. Beide erscheinen in den Top 10 unserer Liste, allerdings ist der prozentuale Anteil aktiver Domains, die mit Botnet C&Cs assoziiert werden, bei einem deutlich höher als beim anderen.

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.

Kooperation mit der Industrie für mehr Sicherheit im Internet

Natürlich wäre es uns am liebsten, wenn es gar keine TLDs gäbe, die mit Botnet C&Cs in Verbindung gebracht werden. Da wir jedoch in der realen Welt leben, bleibt das leider Wunschdenken.

Wichtig ist es jedoch, schnell auf Missbrauch zu reagieren. Wenn Domain-Namen nur zu dem Zweck registriert werden, Malware zu verbreiten oder Botnet C&Cs zu hosten, ist uns daran gelegen, dass die Registrierungsstellen diese Domain-Namen so schnell wie möglich aussetzen. Dabei wissen wir die Bemühungen vieler Registrierungsstellen wie u. a. .xyz und .top zu schätzen, die mit uns zusammenarbeiten, um die entsprechenden Maßnahmen einzuleiten.

Neuzugänge

xxx (Platz 4), site (14), one (15), gq (16), sbs (18), de (20).

Abgänge

cn, su, club, eu, co, monster.

Die am häufigsten missbrauchten TLDs – Anzahl der Domains

Rang	Q3-2021	Q4-2021	% Veränderung	TLD	Typ
1.	3730	3719	-0,2 %	com	gTLD
2.	829	715	-14 %	top	gTLD
3.	833	396	-52 %	xyz	gTLD
4.	-	223	Neuzugang	xxx	gTLD
5.	132	143	8 %	ga	Ursprünglich ccTLD, jetzt effektiv gTLD
6.	665	136	-80 %	net	gTLD
7.	330	133	-60 %	ru	ccTLD
8.	183	122	-33 %	tk	Ursprünglich ccTLD, jetzt effektiv gTLD
9.	265	116	-56 %	org	gTLD
10.	538	108	-80 %	buzz	gTLD
11.	178	103	-42 %	info	gTLD
12.	98	97	-1 %	cf	Ursprünglich ccTLD, jetzt effektiv gTLD
13.	123	87	-29 %	ml	Ursprünglich ccTLD, jetzt effektiv gTLD
14.	-	75	Neuzugang	site	gTLD
15.	-	70	Neuzugang	one	gTLD
16.	-	56	Neuzugang	gq	Ursprünglich ccTLD, jetzt effektiv gTLD
17.	82	52	-37 %	cloud	gTLD
18.	-	51	Neuzugang	sbs	gTLD
19.	170	45	-74%	br	ccTLD
20.	-	44	Neuzugang	de	ccTLD

Am häufigsten missbrauchte Domain-Registrierungsstellen, Q4-2021

Insgesamt verzeichneten wir im 4. Quartal 2021 einen Rückgang der Registrierungen betrügerischer Domains – eine positive Entwicklung, wie wir finden. Doch einige Registrierungsstellen haben immer noch erkennbare Schwierigkeiten.

Registrierungsstellen in Kanada

Registrierungsstellen in Kanada waren im 4. Quartal mit den meisten betrügerischen Botnet-C&C-Registrierungen verbunden und überholten sogar den Spitzenreiter China aus Q3.

Registrierungsstellen in Deutschland

Mit 136 % gab es einen erheblichen Anstieg von Botnet C&Cs, die zu Registrierungsstellen in Deutschland gehören. Dieser Anstieg kam vor allem von Key Systems (Zunahme um 74 %) und 1API, die auf Platz 12 wieder in unsere Rangliste einstiegen, nachdem sie in Q2 zunächst aus den Top 20 verschwunden waren.

Atak

Diese Domain-Registrierungsstelle ist erstmalig in unseren Ranglisten vertreten. Atak wird in der Türkei betrieben und hat bisher nicht auf unsere Missbrauchsmeldungen reagiert. Daher haben wir bei der ICANN eine Beschwerde eingereicht. Es ist unabdingbar, dass alle Akteure im Internet zum Schutz der Internetnutzer zusammenarbeiten.

Nicenic.net (China) und PDR (Indien)

Diese Registrierungsstellen verzeichneten im 4. Quartal einen kräftigen Anstieg der bei ihnen registrierten Botnet C&C-Domains. Doch auch bei steigenden Registrierungszahlen reagiert PDR blitzschnell auf Missbrauchsmeldungen.

Ein Dankeschön an die Abgänge

Im vergangenen Quartal wiesen wir darauf hin, dass bei CentralNic, West263 und Network Solutions ein erheblicher Anstieg neu registrierter Botnet C&C-Domains zu beobachten war. Erfreulicherweise sind diese drei Registrierungsstellen im 4. Quartal zusammen mit eName, Xin Net, 22net und OVH aus unsere Top 20 verschwunden. Herzlichen Glückwunsch zur erfolgreichen Missbrauchsbekämpfung.

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

1API (Platz 12), Beget (14), Sav.com (15), Hostinger (16), Atak (18), Naunet (19), EuroDNS (20),
Mat Bao Corporation (20).

Abgänge

eName, CentralNic, Network Solutions, Xin Net, west263.com, 22net, OVH.

Am häufigsten missbrauchte Domain-Registrierungsstellen, Q4-2021 (Fortsetzung)

Am häufigsten missbrauchte Domain-Registrierungsstellen – Anzahl der Domains

Rang	Q3-2021	Q4-2021	% Veränderung	Registrierungsstelle	Land
1.	1568	988	-37 %	NameSilo	Kanada
2.	1267	718	-43 %	Namecheap	USA
3.	209	536	156 %	nicenic.net	China
4.	169	433	156 %	PDR	Indien
5.	188	328	74 %	Key Systems	Deutschland
6.	154	272	77 %	WebNic.cc	Singapur
7.	1217	201	-83 %	Alibaba	China
8.	165	197	19 %	Openprovider	Niederlande
9.	189	135	-29 %	Eranet International	China
10.	403	127	-68 %	Tucows	Kanada
11.	475	124	-74%	RegRU	Russland
12.	-	115	Neuzugang	1API	Deutschland
13.	403	80	-80 %	Porkbun	USA
14.	-	68	Neuzugang	Beget LLC	Russland
15.	-	66	Neuzugang	Sav.com	USA
16.	-	57	Neuzugang	Hostinger	Litauen
17.	214	54	-75 %	dnspod.cn	China
18.	-	51	Neuzugang	Atak	Türkei
19.	-	49	Neuzugang	NauNet	Russland
20.	-	48	Neuzugang	Mat Bao Corporation	Vietnam
20.	-	48	Neuzugang	EuroDNS	Luxemburg

Standort der am häufigsten missbrauchten Domain-Registrierungsstellen

Land	Botnets	%
Kanada	1115	23,75 %
China	926	19,72 %
USA	864	18,40 %
Deutschland	443	9,44 %
Indien	433	9,22 %
Singapur	272	5,79 %
Russland	241	5,13 %
Niederlande	197	4,20 %
Litauen	57	1,21 %
Türkei	51	1,09 %
Luxemburg	48	1,02 %
Vietnam	48	1,02 %
Gesamt	**4695**	

Netzwerke, welche die meisten neu erkannten Botnet C&Cs hosten, Q4-2021

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“.

Eine bunte Mischung

Uninet.net.mx (Platz 1), serverion.com (5) und cloudflare.com (9) – alle drei erscheinen in den Top 10 unserer Listen, doch unterscheiden sie sich erheblich voneinander.

Uninet ist ein Telekommunikations- und Netzwerkbetreiber in Mexiko. Alle neu gehosteten Botnet C&Cs, die wir in dessen IP-Raum identifizieren konnten, waren auf beeinträchtigte Kundengeräte zurückzuführen.

Serverion ist eine in den Niederlanden ansässige Hosting-Firma. Alle während Q4 in deren Netzwerk identifizierten Botnet C&Cs waren auf betrügerische Registrierungen zurückzuführen.

Zu guter Letzt ist da noch Cloudflare, die keine Inhalte hosten, sondern einen Reverse-Proxy-Service und DDoS-Schutz für Botnet C&Cs bietet, um deren wahren Standort zu verbergen.

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

selectel.ru (Platz 10), timeweb.ru (12), firstbyte.ru (13), pinvds.com (15), ihor-hosting.ru (18), itldc.com (19), m247.ro (20).

Abgänge

ipjetable.net, pq.hosting, ovh.com, mivocloud.com, telefonica.com.ar, uplus.co.kr, mgnhost.ru.

Netzwerke, welche die meisten neu erkannten Botnet C&Cs hosten, Q4-2021 (Fortsetzung)

Neu erkannte Botnet C&Cs pro Netzwerk

Rang	Q3-2021	Q4-2021	% Veränderung	Netzwerk	Land
1.	177	187	6 %	uninet.net.mx	Mexiko
2.	33	182	452 %	alibaba-inc.com	China
3.	63	175	178 %	antel.net.uy	Uruguay
4.	105	168	60 %	stc.com.sa	Saudi-Arabien
5.	115	116	1 %	serverion.com	Niederlande
6.	95	110	16 %	claro.com.do	Dominikanische Republik
7.	58	85	47 %	telefonica.com.br	Brasilien
8.	44	80	82 %	baxet.ru	Russland
9.	68	72	6 %	cloudflare.com	USA
10.	-	63	Neuzugang	selectel.ru	Russland
11.	44	51	16 %	nano.lv	Lettland
12.	-	49	Neuzugang	timeweb.ru	Russland
13.	-	48	Neuzugang	firstbyte.ru	Russland
13.	33	48	45 %	hostwinds.com	USA
15.	-	47	Neuzugang	pinvds.com	Russland
16.	89	39	-56 %	privacyfirst.sh	Deutschland
17.	51	38	-25 %	hetzner.de	Deutschland
18.	-	36	Neuzugang	ihor-hosting.ru	Russland
19.	-	35	Neuzugang	itldc.com	Ukraine
20.	-	34	Neuzugang	m247.ro	Rumänien

Netzwerke, welche die aktivsten Botnet C&Cs hosten, Q4-2021 (Fortsetzung)

Zum guten Schluss werfen wir noch einen Blick auf die Netzwerke, die Ende 2021 die meisten aktiven Botnet C&Cs gehostet haben. 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

al.bg (Platz 8), mobily.com.sa (12), ielo.net (13), google.com (16), combahton.net (16).

Abgänge

serverion.com, uplus.co.kr, hostry.com, skbroadband.com, claro.com.co.

Dringender Handlungsbedarf bei Netzwerkbetreibern in Lateinamerika

Mehr als 60 % der aktiven Botnet C&C-Einträge betreffen Netzwerke in Lateinamerika. Wir bitten die betroffenen Betreiber dringend, auf Missbrauchsmeldungen zu reagieren und gemeinsam mit Spamhaus die Botnet C&C-Aktivitäten in ihren Netzwerken zu verringern.

Gesamtzahl aktiver Botnet C&Cs pro Netzwerk (Stand: 31. Dezember 2021)

Rang	Q3-2021	Q4-2021	% Veränderung	Netzwerk	Land
1.	185	389	110 %	uninet.net.mx	Mexiko
2.	119	296	149 %	stc.com.sa	Saudi-Arabien
3.	68	257	278 %	antel.net.uy	Uruguay
4.	97	204	110 %	claro.com.do	Dominikanische Republik
5.	63	146	132 %	telefonica.com.br	Brasilien
6.	79	94	19 %	microsoft.com	USA
7.	99	91	-8 %	ipjetable.net	Frankreich
8.	-	60	Neuzugang	a1.bg	Bulgarien
9.	41	41	0 %	telefonica.com.ar	Argentinien
10.	29	29	0 %	tie.cl	Chile
10.	32	29	-9 %	vietserver.vn	Vietnam
12.	-	27	Neuzugang	mobily.com.sa	Saudi-Arabien
13.	-	25	Neuzugang	ielo.net	Frankreich
14.	21	24	14 %	clouvider.net	Großbritannien
15.	24	22	-8 %	ovpn.com	Schweden
16.	22	21	-5 %	charter.com	USA
16.	-	21	Neuzugang	google.com	USA
16.	21	21	0 %	algartelecom.com.br	Brasilien
16.	21	21	0 %	une.net.co	Kolumbien
16.	-	21	Neuzugang	combahton.net	Deutschland