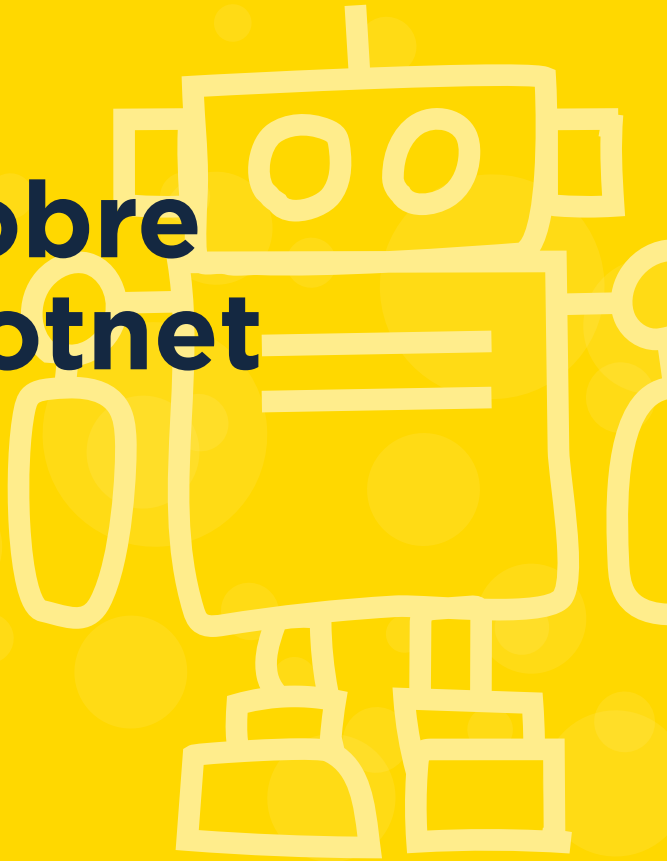
SPAMHAUS



Atualização sobre ameaças de botnet da Spamhaus

T3 2021

O 3º trimestre sentiu um aumento estrondoso de 82% no número de novos comandos e controles (CCs) de botnet identificados por nossa equipe de pesquisadores. Foi observado um aumento repentino no uso de malwares de backdoor pelas mãos de operadores nefastos que se escondem atrás de redes de fluxo rápido (FastFlux). Isso fez com que vários novos países e provedores de serviços entrassem na nossa lista dos Top 20.

Sejam bem-vindos à atualização sobre ameaças de botnet da Spamhaus para o 3º trimestre de 2021.

Sobre este relatório

A Spamhaus rastreia endereços de protocolo de internet (IP) e nomes de domínio usados por agentes de ameaças para hospedar servidores de comando e controle (CC) de botnet. Esses dados permitem que identifiquemos elementos associados, incluindo a geolocalização dos botnet CCs, o malware associado a eles, os domínios de nível superior (TLDs) usados ao registrar um domínio para um botnet CC, e os registradores que patrocinam e a rede que hospeda a infraestrutura do botnet CC.

Este relatório oferece uma visão geral sobre o número de botnet CCs associados a esses elementos, juntamente com uma comparação trimestral. Discutimos as tendências que observamos e destacamos provedores de serviços lutando para controlar o número de operadores de botnet que usam seus serviços indevidamente.

Destaque

A volta das FastFlux

Após analisarmos as estatísticas do trimestre, ficou evidente que as FastFlux estão se popularizando novamente. Eis aqui uma recapitulação rápida sobre as FastFlux, incluindo também uma análise mais profunda sobre o seu uso por cibercriminosos para manter a resiliência de suas infraestruturas maléficas.

O que é FastFlux?

FastFlux é uma técnica usada por phishers, criadores de malware e operadores de botnet para ocultar a real localização da infraestrutura por trás de uma rede de hosts comprometidos que atuam como proxies, encaminhando o tráfego malicioso para o verdadeiro backend.

O que deixa as FastFlux tão atraentes para os cibercriminosos?

Todas as redes FastFlux que estão atualmente em operação podem ser alugadas na dark web como um serviço. Isso facilita muito a vida dos operadores de botnet. Tudo o que eles precisam fazer é registrar os domínios necessários para os botnet CCs e apontá-los para o serviço do operador da FastFlux. A FastFlux cuida do resto, assegurando que os registros A mudem rapidamente.

Temos aqui um exemplo de um domínio de botnet CC FluBot hospedado em uma botnet FastFlux:

```
;; SEÇÃO DE PERGUNTA:
;gurbngbcxheshsj.ru.        IN    A

;; SEÇÃO DE RESPOSTA:
```

Domínio	TTL	Tipo de registro		Endereço IP
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

O que é FluBot?

FluBot é um cavalo de troia que infecta dispositivos Android. Ele rouba as credenciais do usuário e se propaga, transformando o smartphone infectado em um zumbi de spam por SMS.

Como você pode ver, o domínio de botnet CC usa dez registros A simultâneos com uma vida útil (TTL) de apenas 150 segundos. O monitoramento desses registros A revela que a botnet FastFlux em questão consiste em 100 a 150 nós ativos de FastFlux por dia.

Normalmente, esses nós são dispositivos comprometidos, como equipamentos nas instalações do cliente (CPE), configurados de modo não seguro (por exemplo, executando softwares vulneráveis ou usando credenciais de login padrão) e acessíveis diretamente da internet.

Esses tipos de dispositivos são alvo fácil para os cibercriminosos. Eles só precisam fazer varreduras na internet para detectar esses dispositivos vulneráveis e comprometê-los. O processo todo pode ser automatizado, deixando tudo mais rápido, fácil e eficiente.

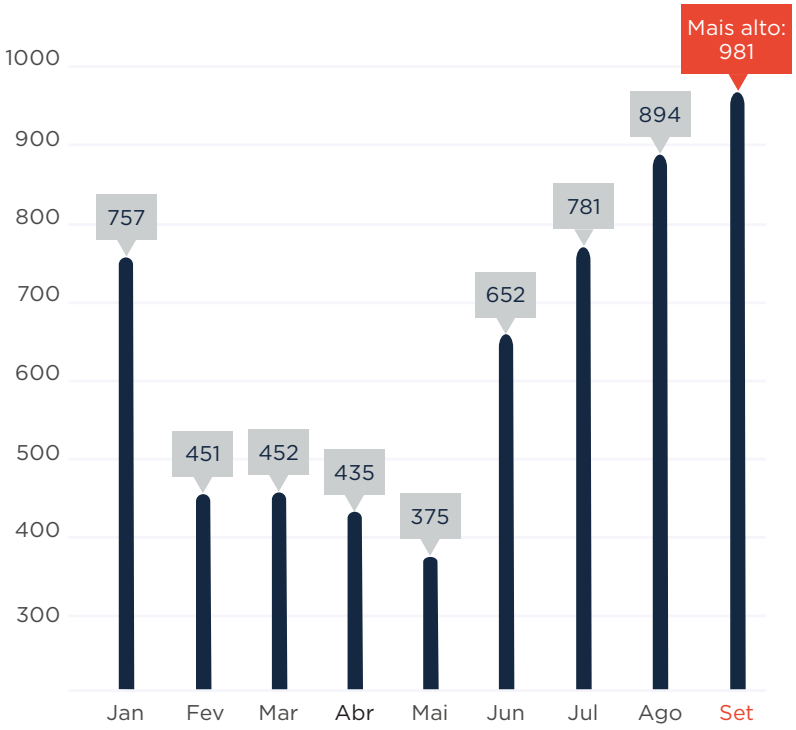
Os operadores de botnets FastFlux escolhem cuidadosamente a localização geográfica dos dispositivos-alvo que usam para hospedar a FastFlux. Como você notará durante a leitura desse relatório, muitos nós CC de FastFlux são hospedados em lugares relativamente bem “digitalizados”, ou seja, com boas conexões de internet, mas que não avançaram na curva de maturidade em termos de segurança cibernética.

A América Latina é um alvo comum, como Brasil, Chile, Argentina e Uruguai, e também os países asiáticos, como a Coreia. Os recém-chegados a esta atualização estatística baseada em geolocalização são a prova disso.

Número de botnet CCs observados, T3 2021

No 3º trimestre de 2021, a Spamhaus Malware Labs identificou 2.656 botnet CCs em comparação com 1.462 no 2º trimestre de 2021. Esse foi um aumento de 82% entre trimestres! A média mensal de botnet CCs subiu de 487 por mês no T2 para 885 botnet CCs por mês no T3.

Número de novos botnet CCs detectados pela Spamhaus em 2021:



Trimestre	Nº de botnets	Média trimestral	Mudança %
T1	1660	553	24%
T2	1462	487	-12%
T3	2656	885	82%

O que são controladores de botnet?

"Servidor de comando e controle de botnet", "controlador de botnet" ou "botnet C2" são maneiras comuns de nos referirmos ao "botnet CC". Os fraudadores usam essa rede para controlar computadores infectados por malware e extrair valiosos dados pessoais das vítimas infectadas pelo malware.

Os botnet CCs desempenham um papel vital nas operações realizadas por cibercriminosos que usam computadores infectados para enviar spam ou ransomware, lançar ataques DDoS, aplicar golpes relacionados a bancos eletrônicos ou click fraud, ou minerar criptomoedas, como bitcoins.

Computadores de mesa e dispositivos móveis, como smartphones, não são os únicos equipamentos que podem ser infectados. O número de dispositivos conectados à internet aumenta a cada dia, por exemplo, os dispositivos de Internet das Coisas (IoT), como webcams, unidades de armazenamento de dados em rede (NAS) e muitos outros. Eles também correm o risco de serem infectados.

Geolocalização de botnet CCs, T3 2021

Dada a influência das FastFlux durante o último trimestre, não surpreende que haja um claro padrão que delineia os que passaram a integrar o gráfico do 3º trimestre de 2021. Muitos dos países que agora despontam nos gráficos foram responsáveis por hospedar uma alta porcentagem de TeamBot e servidores de botnet CC FluBot — utilizando FastFlux —, e se enquadram no perfil de países com grande cobertura de internet, porém com pouco foco em segurança.

Aumentos significativos na Rússia

O número de botnet CCs localizados na Rússia aumentou drasticamente. Esse é o segundo aumento trimestral que a Rússia enfrenta:

- T1 para T2 – 19% de aumento
- T2 para T3 – 64% de aumento

Portanto, não surpreende que no 3º trimestre a Rússia tenha ultrapassado os EUA e assumido a primeira posição.

Aumento contínuo na Europa

A tendência do T2 continuou no T3. Mais uma vez, houve um aumento no número de servidores de botnet CC hospedados em vários países europeus, incluindo Países Baixos (+63%), Alemanha (+45%), França (+34%) e Suíça (+34%).

Novas entradas

México (nº 4), Arábia Saudita (nº 7), República Dominicana (nº 8), Coreia (nº 10), Uruguai (nº 11), Argentina (nº 14), Suécia (nº 18), Romênia (nº 20).

Partidas

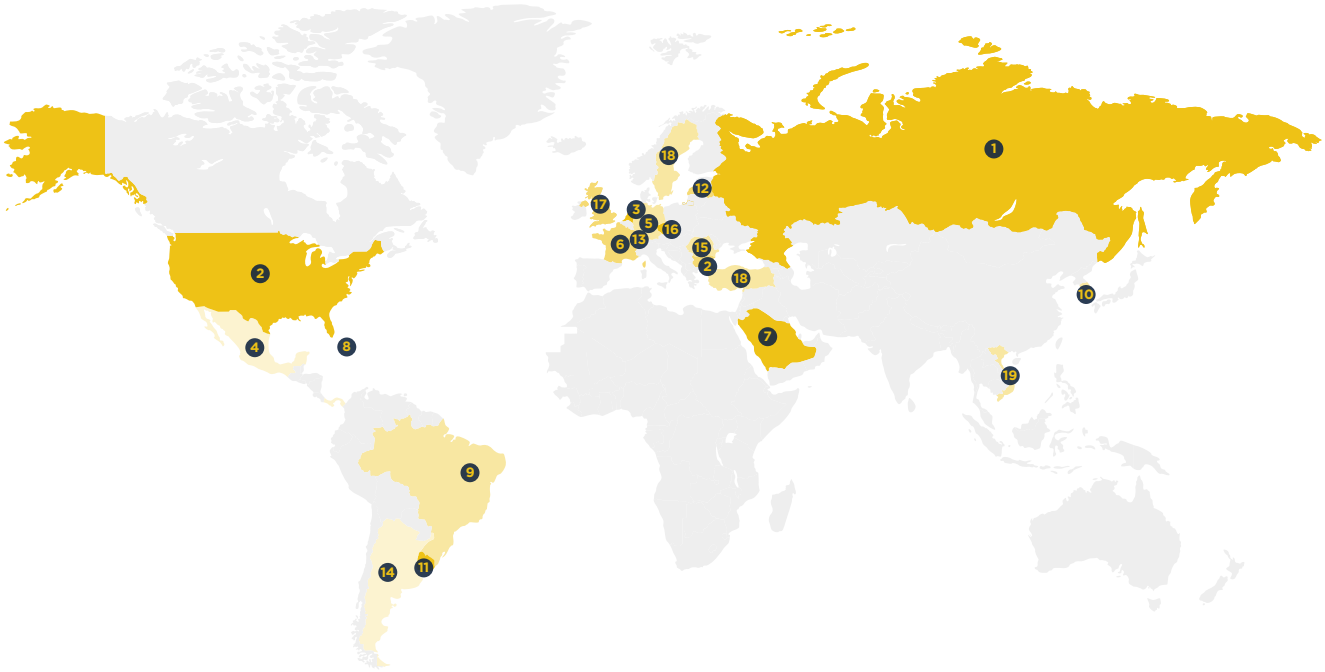
Ucrânia, Seychelles, Panamá, Canadá, Malásia, Polônia, Finlândia, Turquia.

Geolocalização de botnet CCs, T3 2021 (continuação)

Top 20 localizações de botnet CCs

Posição	País	T2 2021	T3 2021	Mudança % T a T
Nº 1	Rússia	233	381	64%
Nº 2	Estados Unidos	281	301	7%
Nº 3	Países Baixos	168	273	63%
Nº 4	México	-	182	Nova entrada
Nº 5	Alemanha	117	170	45%
Nº 6	França	92	123	34%
Nº 7	Arábia Saudita	-	117	Nova entrada
Nº 8	Rep. Dominicana	-	96	Nova entrada
Nº 9	Brasil	12	86	617%
Nº 10	Coreia	-	68	Nova entrada

Posição	País	T2 2021	T3 2021	Mudança % T a T
Nº 11	Uruguai	-	63	Nova entrada
Nº 12	Letônia	84	58	-31%
Nº 13	Suíça	41	55	34%
Nº 14	Argentina	-	50	Nova entrada
Nº 15	Moldávia	29	49	69%
Nº 16	República Tcheca	31	40	29%
Nº 17	Reino Unido	57	39	-32%
Nº 18	Suécia	-	38	Nova entrada
Nº 19	Vietnã	13	34	162%
Nº 20	Romênia	-	33	Nova entrada



Malware associado a botnet CCs, T3 2021

Descrevemos aqui as principais famílias de malwares associados a botnet CCs recém-observados no T3 2021.

O surgimento do TeamBot e do FluBot

Você já ouviu falar do TeamBot? Provavelmente não. Ainda que não seja uma ameaça nova nem seja grave, o TeamBot aparece no topo da lista junto com o FluBot, ambos backdoors.

Nossos caçadores de ameaças acreditam que o TeamBot e o FluBot usam a mesma infraestrutura de FastFlux, circulando os mesmos endereços IP de botnet CC a pequenos intervalos de tempo, por isso o posicionamento compartilhado na lista abaixo.

Neste trimestre, houve um aumento repentino no número de malwares de backdoor, fazendo deles o tipo mais predominante de malware associado a botnet CCs no 3º trimestre de 2021.

RedLine vence, Raccoon perde

Em 2021, temos observado uma batalha pela *pole position* entre RedLine e Raccoon, ambos ladrões de credenciais que se encontram à venda na dark web. Embora tenhamos visto um aumento considerável (571%) em servidores do botnet CC Raccoon no T2 2021, o malware RedLine mostrou um aumento de 71% no T3 2021, desbancando o Raccoon de sua posição.

IcedID desaparece

O IcedID tem se mantido relativamente inativo este ano, fazendo uma breve aparição na posição nº 18 no 2º trimestre, antes de sumir de novo neste trimestre. O motivo disso é desconhecido. Contudo, nossos pesquisadores não acreditam que esse silêncio se manterá indefinidamente. O IcedID é um dos cavalos de troia disponíveis para grupos de ransomware para compra na dark web. Esses cavalos de troia vendem acesso a redes corporativas, um negócio bastante lucrativo.

O que é malware de backdoor?

Este tipo de malware rodeia os procedimentos normais de autenticação e outras medidas de segurança para obter acesso de alto nível a um sistema, rede ou aplicativo.

Novas entradas

TeamBot (nº 1), FluBot (nº 1) Smoke Loader (nº 9), AveMaria (nº 13).

Partidas

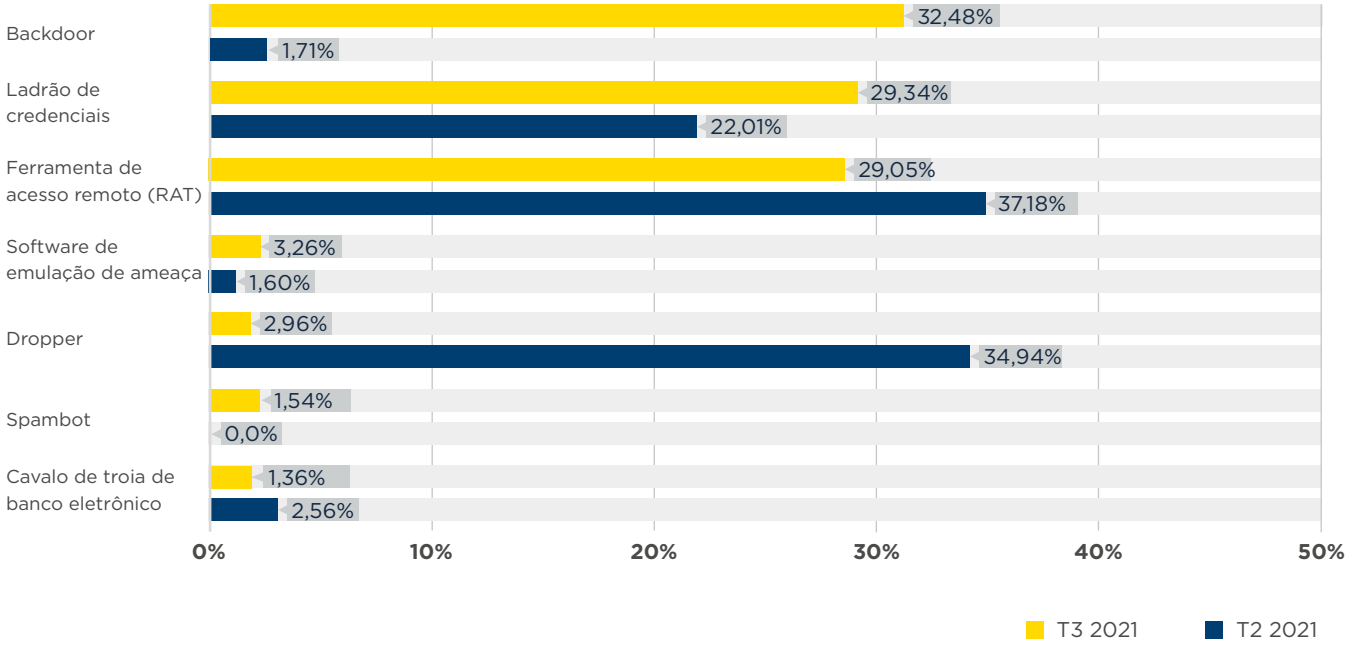
Oski, IcedID, Arkei.

Malware associado a botnet CCs, T3 2021 (continuação)

Famílias de malware associadas a botnet CCs

Posição	T2 2021	T3 2021	Mudança %	Família de malware	Descrição
Nº 1	-	507	Nova entrada	TeamBot & FluBot	Backdoor
Nº 2	123	210	71%	RedLine	Ladrão de credenciais
Nº 3	42	136	224%	BitRAT	Ferramenta de acesso remoto (RAT)
Nº 4	83	121	46%	AsyncRAT	Ferramenta de acesso remoto (RAT)
Nº 5	66	108	64%	Loki	Ladrão de credenciais
Nº 6	302	93	-69%	Raccoon	Ladrão de credenciais
Nº 7	24	71	196%	NjRAT	Ferramenta de acesso remoto (RAT)
Nº 8	15	55	267%	Cobalt Strike	Backdoor
Nº 9	-	50	Nova entrada	Smoke Loader	Dropper
Nº 10	26	43	65%	VjwOrm	Ladrão de credenciais
Nº 11	16	41	156%	CryptBot	Backdoor
Nº 12	24	40	67%	RemcosRAT	Ferramenta de acesso remoto (RAT)
Nº 13	-	37	Nova entrada	AveMaira	Ferramenta de acesso remoto (RAT)
Nº 13	23	37	61%	NanoCore	Ferramenta de acesso remoto (RAT)
Nº 15	17	30	76%	STRRAT	Ferramenta de acesso remoto (RAT)
Nº 16	23	26	13%	Tofsee	Spambot
Nº 17	14	24	71%	ServHelper	Ladrão de credenciais
Nº 18	43	23	-47%	Gozi	Cavalo de troia de banco eletrônico
Nº 19	11	18	64%	QuasarRAT	Ferramenta de acesso remoto (RAT)
Nº 20	23	17	-26%	AgentTesla	Ladrão de credenciais

Comparações de tipos de malware entre T2 e T3 2021



Domínios de nível superior (TLDs) mais explorados, T3 2021

Sem mudanças no placar

No 3º trimestre, .com e .xyz mantiveram a liderança no nosso ranking. A situação deteriorou para esses dois TLDs, particularmente para o .com, que sentiu um aumento de 90%. Esperamos que a VeriSign e a XYZ.COM, proprietárias desses TLDs, tomem as medidas necessárias para resolver essa situação e melhorar a reputação de seus TLDs.

Três novos TLDs

Dois novos gTLDs e um ccTLD se juntaram aos nossos Top 20: .club, .co e .monster. Todos mostraram um aumento significativo no número de novos domínios de botnet CC registrados através de seus serviços.

Domínios de nível superior (TLDs) — uma breve apresentação

Existem vários domínios de nível superior (TLDs) diferentes, incluindo:

TLDs genéricos (gTLDs)
Podem ser usados por qualquer um.

TLDs de código de país (ccTLDs)
Alguns ccTLDs têm uso restrito em um determinado país ou região, entretanto, outros são licenciados para uso geral, tendo a mesma funcionalidade dos gTLDs.

TLDs descentralizados (dTLDs)
Domínios de nível superior (TLDs) independentes que não estão sob o controle da ICANN.

Novas entradas

club (nº 9), co (nº 18), monster (nº 19).

Partidas

vip, online, live.

Domínios de nível superior (TLDs) mais explorados, T3 2021 (continuação)

TLDs mais explorados — número de domínios

Posição	T2 2021	T3 2021	Mudança %	TLD	Observação
Nº 1	4113	7827	90%	com	gTLD
Nº 2	739	833	13%	xyz	gTLD
Nº 3	607	829	37%	top	gTLD
Nº 4	146	665	355%	net	gTLD
Nº 5	662	538	-19%	buzz	ccTLD
Nº 6	151	330	119%	ru	ccTLD
Nº 7	139	306	120%	cn	ccTLD
Nº 8	157	265	69%	org	gTLD
Nº 9	140	183	31%	tk	Originalmente ccTLD, agora efetivamente gTLD
Nº 9	80	183	129%	su	ccTLD
Nº 9	-	183	Nova entrada	club	gTLD
Nº 12	78	178	128%	info	gTLD
Nº 13	208	170	-18%	br	ccTLD
Nº 14	106	132	25%	ga	Originalmente ccTLD, agora efetivamente gTLD
Nº 15	116	126	9%	eu	ccTLD
Nº 16	104	123	18%	ml	Originalmente ccTLD, agora efetivamente gTLD
Nº 17	73	98	34%	cf	ccTLD
Nº 18	-	89	Nova entrada	co	ccTLD
Nº 19	-	82	Nova entrada	monster	gTLD
Nº 19	141	82	-42%	cloud	gTLD

Registradores de domínios mais explorados, T3 2021

Observamos aumentos significativos entre a maioria dos registradores de domínios listados no nosso Top 20. A China abriga a maior porcentagem de registradores de domínios, seguida pelo Canadá e pelos Estados Unidos. Ainda que o índice percentual do Canadá e da Índia tenha caído, muitos outros países listados mostraram um aumento neste trimestre*.

No T2, você viu o Arsys, agora não vê mais

Cumprimentos ao Arsys, que apareceu como uma nova entrada no 2º trimestre, ocupando a 5ª posição. Parece que eles tomaram medidas positivas para garantir que o TLD se mantivesse o mais limpo possível e saíram do Top 20 no T3, juntamente com HiChina, 1API, Name.com e 55hl.com. Um excelente trabalho por parte desses registradores.

Problemas na distribuição

No 3º trimestre, vimos o maior aumento em domínios de botnet CC recém-registrados no CentralNic (+488%), Tucows (+266%), RegRU (+252%), West263.com (+168%) e Network Solutions (+163%).

A grande maioria dos registros de nomes de domínios fraudulentos se origina de revendedores sem um sistema de avaliação adequado ou que simplesmente não fazem nenhuma averiguação dos clientes.

Os registradores podem enfrentar dificuldades para penalizar esses revendedores de má-fé por diversos motivos, inclusive Termos de Serviços (ToS) mal redigidos. Contudo, outros fatores também podem entrar na equação, como interesses financeiros adquiridos ou uma falta fundamental de motivação para assumir a responsabilidade pelos problemas.

Esperamos que esses registradores melhorem sua reputação rapidamente, implementando medidas mais rigorosas na distribuição por seus revendedores para intensificar a luta contra o registro de nomes de domínios fraudulentos.

Registradores e operadores de botnet CC

Os cibercriminosos precisam encontrar um registrador patrocinador para conseguirem registrar um nome de domínio para botnet CC. Não é fácil para os registradores detectarem todos os registros fraudulentos antes que esses domínios entrem em atividade. Entretanto, o "tempo de vida" de domínios criminosos em um registrador legítimo e bem-estruturado costuma ser relativamente curto.

Novas entradas

Porkbun (nº 7), dnspod.cn (nº 11), nicenic.net (nº 13), Openprovider (nº 18), OVH (nº 19).

Partidas

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

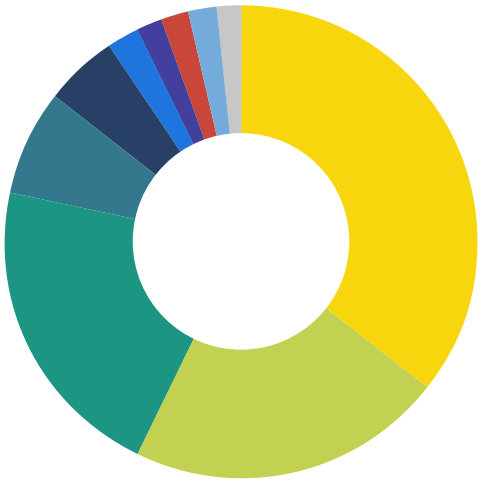
* Atualizado em 15 de outubro de 2021 | Dois registradores (NameSilo e Tucows) foram listados como provedores sediados nos EUA quando este relatório foi originalmente publicado. Atualizamos o texto e os dados de modo a refletir que eles estão sediados no Canadá.

Registradores de domínios mais explorados, T3 2021 (continuação)

Registradores de domínios mais explorados — número de domínios

Posição	T2 2021	T3 2021	Mudança %	Registrador	País
Nº 1	1797	1568	-13%	NameSilo	Canadá*
Nº 2	955	1267	33%	Namecheap	Estados Unidos
Nº 3	504	1217	141%	Alibaba	China
Nº 4	526	787	50%	eName Technology	China
Nº 5	112	658	488%	CentralNic	Reino Unido
Nº 6	135	475	252%	RegRU	Rússia
Nº 7	110	403	266%	Tucows	Canadá*
Nº 7	-	403	Nova entrada	Porkbun	Estados Unidos
Nº 9	101	266	163%	Network Solutions	Estados Unidos
Nº 10	125	255	104%	Xin Net	China
Nº 11	80	214	168%	west263.com	China
Nº 11	-	214	Nova entrada	dnspod.cn	China
Nº 13	-	209	Nova entrada	nicenic.net	China
Nº 14	215	189	-12%	Eranet International	China
Nº 15	92	188	104%	Key Systems	Alemanha
Nº 16	110	176	60%	22net	China
Nº 17	188	169	-10%	PDR	Índia
Nº 18	-	165	Nova entrada	Openprovider	Países Baixos
Nº 19	-	160	Nova entrada	OVH	França
Nº 20	91	154	69%	WebNic.cc	Singapura

LOCALIZAÇÃO DOS REGISTRADORES DE DOMÍNIOS MAIS EXPLORADOS



País	Botnets	%
China	3261	35,7%
Canadá*	1971	21,57%
Estados Unidos	1936	21,19%
Reino Unido	658	7,2%
Rússia	475	5,2%
Alemanha	188	2,1%
Índia	169	1,8%
Países Baixos	165	1,8%
França	160	1,8%
Singapura	154	1,7%
Total	**9137**	

* Atualizado em 15 de outubro de 2021 | Dois registradores (NameSilo e Tucows) foram listados como provedores sediados nos EUA quando este relatório foi originalmente publicado. Atualizamos o texto e os dados de modo a refletir que eles estão sediados no Canadá.

Redes que hospedam os mais novos botnet CCs recém-observados, T3 2021

Como de costume, ocorreram muitas mudanças nas redes que hospedam botnet CCs recém-observados. É interessante notar que houve um influxo de redes hospedando botnet CCs FastFlux, usados pelos cibercriminosos para hospedar malwares de backdoor.

Esta lista reflete a rapidez com que o problema de abuso é tratado nas redes?

Ainda que a lista das Top 20 ilustre que talvez haja um problema com o processo de averiguação dos clientes, ela não reflete a velocidade com que o pessoal de triagem lida com as denúncias recebidas de uso indevido. Consulte "Redes que hospedam os botnet CCs mais ativos" para ver em quais redes os abusos não são tratados com rapidez.

serverion.com

Vimos um aumento de 69% no número de novos servidores de botnet CC instalados no provedor de hospedagem holandês serverion.com. Nossos pesquisadores acreditam que esse aumento se deva, sobretudo, a um cliente em sua cadeia, des.capital, que costuma atrair operadores de botnet.

Mudanças positivas

Na atualização do último trimestre, divulgamos que a operação de hospedagem de botnets havia mudado da Amazon para a DigitalOcean, fazendo com que essa última disparasse no placar.
Queremos parabenizar a DigitalOcean por sair da nossa lista das Top 20 no T3 2021, além de outras redes, incluindo a Google, que estava na 2ª colocação, e a HostSailor, a Microsoft, a M247 e a Off Shore Racks.

Redes e operadores de botnet CC

As redes têm um controle razoável sobre os operadores que se cadastram fraudulentamente para receber um novo serviço.

Um processo de averiguação/avaliação deveria ser aplicado antes de autorizar um serviço.

Quando as redes apresentam um grande número de entradas, isso ressalta um dos seguintes problemas:

1. As redes não estão seguindo as boas práticas no processo de averiguação do cliente.
2. As redes não estão assegurando que TODOS os seus revendedores sigam práticas sólidas de averiguação de clientes.

Em alguns dos piores cenários, funcionários ou proprietários de redes se beneficiam diretamente dos cadastros fraudulentos, ou seja, recebem dinheiro deliberadamente dos meliantes em troca da hospedagem de seus botnet CCs; felizmente, isso não acontece com muita frequência.

Novas entradas

uninet.net.mx (nº 1), stc.com.sa (nº 3), claro.com.do (nº 4), antel.net.uy (nº 8), telefonica.com.br (nº 9), telefonica.com.ar (nº 16), uplus.co.kr (nº 17), hotwinds.com (nº 18).

Partidas

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

Redes que hospedam os mais novos botnet CCs recém-observados, T3 2021 (continuação)

Botnet CCs recém-observados por rede

Posição	T2 2021	T3 2021	Mudança %	Rede	País
Nº 1	-	177	Nova entrada	uninet.net.mx	México
Nº 2	68	115	69%	serverion.com	Países Baixos
Nº 3	-	105	Nova entrada	stc.com.sa	Arábia Saudita
Nº 4	-	95	Nova entrada	claro.com.do	Rep. Dominicana
Nº 5	48	89	85%	privacyfirst.sh	Alemanha
Nº 6	35	69	97%	ipjetable.net	França
Nº 7	29	68	134%	cloudflare.com	Estados Unidos
Nº 8	-	63	Nova entrada	antel.net.uy	Uruguai
Nº 9	-	58	Nova entrada	telefonica.com.br	Brasil
Nº 10	82	56	-32%	pq.hosting	Rússia
Nº 11	56	52	-7%	ovh.com	França
Nº 12	46	51	11%	hetzner.de	Alemanha
Nº 13	16	45	181%	mivocloud.com	Moldávia
Nº 14	40	44	10%	baxet.ru	Rússia
Nº 14	49	44	-10%	nano.lv	Letônia
Nº 16	-	43	Nova entrada	telefonica.com.ar	Argentina
Nº 17	-	41	Nova entrada	uplus.co.kr	Coreia
Nº 18	26	33	27%	alibaba-inc.com	China
Nº 18	-	33	Nova entrada	hotwinds.com	Estados Unidos
Nº 20	47	32	-32%	mgnhost.ru	Rússia

Redes que hospedam os botnet CCs mais ativos, T3 2021

Para finalizar, vamos dar uma olhada nas redes que hospedaram um grande número de botnet CCs ativos no 3º trimestre de 2021. Os provedores de hospedagem que aparecem nessa classificação têm um problema de exploração ou não tomam as medidas cabíveis quando recebem denúncias de uso indevido.

Um aumento no uso abusivo por botnet CC

Infelizmente, a situação em termos de servidores de botnet CC ativos deteriorou para muitos ISPs que estavam na nossa lista dos Top 20 no T2. Ipjetable.net (FR), microsoft.com (US), vietserver.vn (VN) e openvpn (SE) têm uma coisa em comum: em vez de tomarem as medidas necessárias contra o uso indevido de suas infraestruturas, o número de servidores de botnet CC ativos aumentou em suas redes.

uninet.net.mx e stc.com.sa

Esses dois ISPs são novos no nosso Top 20 deste trimestre, assumindo a 1ª e 2ª posições devido ao vasto número de bots FastFlux hospedados em suas redes.

Na verdade, a maioria dos recém-chegados ao gráfico está ali por hospedar bots FastFlux em suas redes e não responder rapidamente às denúncias de abuso. Todas essas empresas estão proporcionando uma infraestrutura de botnet CC resiliente para os operadores de botnet.

Novas entradas

uninet.net.mx (nº 1), stc.com.sa (nº 2), claro.com.do (nº 4), antel.net.uy (nº 6), telefonica.com.br (nº 7), telefonica.com.ar (nº 8), tie.cl (nº 10), serverion.com (nº 10), algartelecom.com.br (nº 14), uplus.co.kr (nº 17), skbroadband.com (nº 19).

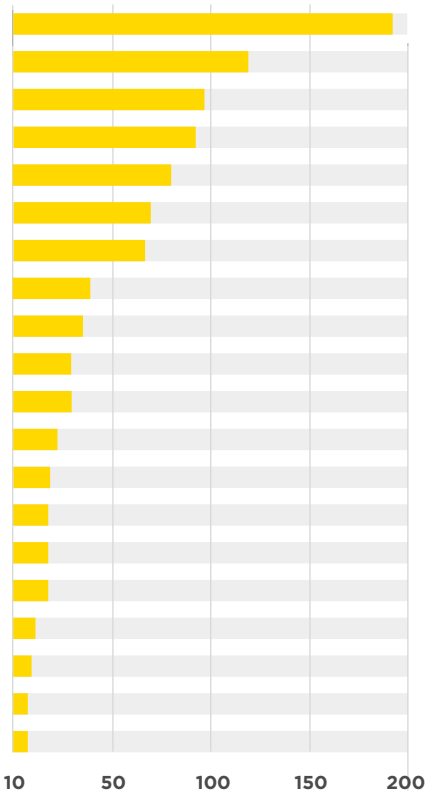
Partidas

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

Redes que hospedam os botnet CCs mais ativos, T3 2021 (continuação)

Número total de botnet CCs ativos por rede

Posição	T2 2021	T3 2021	Mudança %	Rede	País
Nº 1	-	185	Nova entrada	uninet.net.mx	México
Nº 2	-	119	Nova entrada	stc.com.sa	Arábia Saudita
Nº 3	61	99	62%	ipjetable.net	França
Nº 4	-	97	Nova entrada	claro.com.do	Rep. Dominicana
Nº 5	58	79	36%	microsoft.com	Estados Unidos
Nº 6	-	68	Nova entrada	antel.net.uy	Uruguai
Nº 7	-	63	Nova entrada	telefonica.com.br	Brasil
Nº 8	-	41	Nova entrada	telefonica.com.ar	Argentina
Nº 9	23	32	39%	vietserver.vn	Vietnã
Nº 10	-	29	Nova entrada	tie.cl	Chile
Nº 10	-	29	Nova entrada	serverion.com	Países Baixos
Nº 12	20	24	20%	ovpn.com	Suécia
Nº 13	21	22	5%	charter.com	Estados Unidos
Nº 14	-	21	Nova entrada	algartelecom.com.br	Brasil
Nº 14	18	21	17%	cloudvider.net	Reino Unido
Nº 14	17	21	24%	une.net.co	Colômbia
Nº 17	-	19	Nova entrada	uplus.co.kr	Coreia
Nº 18	17	18	6%	hostry.com	Chipre
Nº 19	-	17	Nova entrada	skbroadband.com	Coreia
Nº 19	12	17	42%	claro.com.co	Colômbia



Por enquanto, é isso.

Protejam-se, e nos vemos em janeiro!