



INDICATEURS CLÉS DU RAPPORT NETSCOUT SUR LES CYBERMENACES (THREAT INTELLIGENCE REPORT) POUR LE S1 2021

FRANCE



Le transfert massif vers la vie en ligne, déclenché par la pandémie de COVID-19, a entraîné des niveaux d'innovation record par les acteurs malveillants, et l'équipe d'intervention et d'ingénierie de sécurité ATLAS (ASERT) de NETSCOUT prévoit que cette innovation prolongée de la part des cybercriminels se prolongera encore longtemps dans l'année 2021.

Les acteurs malveillants ont lancé environ 5,4 millions d'attaques DDoS pendant le S1 2021, là aussi un chiffre record. En particulier, ils ont lancé des nombres sans précédent d'attaques DDoS au cours du premier trimestre, en augmentant la fréquence de ces attaques de 20 % par rapport à la même période en 2020. Pendant ce temps, des adversaires ont découvert ou transformé en armes sept vecteurs d'attaques DDoS par réflexion/amplification UDP, et ils ont développé des attaques multivecteurs adaptatives spécialement ajustées pour tirer profit des vulnérabilités de leurs victimes. Des composants essentiels de la chaîne d'approvisionnement de la connectivité ont subi des attaques accrues, alors que des gangs de rançongiciels ont ajouté à leur répertoire des tactiques DDoS de triple extorsion et que l'acteur malveillant Fancy Lazarus lançait une nouvelle campagne d'extorsion par DDoS.

Max. d'une attaque multivecteur

Nombre max. de vecteurs au cours d'une même attaque

22

VECTEURS D'ATTAQUE UTILISÉS

1. Amplification Chargen
2. Amplification COAP
3. DNS
4. Amplification DNS
5. ICMP
6. ISAKMP
7. Amplification Jenkins
8. Amplification Memcached
9. Amplification MSSQLRS
10. Amplification NetBIOS
11. Amplification NTP
12. Amplification RIPv1
13. Amplification Sentinel
14. Amplification SIP
15. Amplification SNMP
16. Amplification SSDP
17. Amplification STUN
18. TCP ACK
19. TCP NULL
20. TCP RST
21. TCP SYN
22. Amplification TCP SYN/ACK

Top 5 des vecteurs d'attaque

Ta TCP ACK	Dn Amp. DNS	Ts TCP SYN	Tr TCP RST	Ds DNS
NOMBRE D'ATTAQUES 16 705	NOMBRE D'ATTAQUES 14 938	NOMBRE D'ATTAQUES 14 066	NOMBRE D'ATTAQUES 12 654	NOMBRE D'ATTAQUES 12 483

Statistiques DDoS

Fréquence des attaques	-48 %
Débit max.	-45 %
Durée moyenne	+29 %
Ampleur max. des attaques	-16 %

Attaque la plus intense

Ampleur	222,76 Gbps
Vitesse	26,45 Mpps
Durée	7 915 s

Débit de pointe max.

Date	06/01/2021
Débit max.	139 Mpps

Bande passante de pointe max.

Date	05/01/2021
Bande passante max.	285 Gbps



Top dix des industries verticales ciblées

Le tableau ci-dessous présente un échantillon des secteurs les plus touchés au cours du S1 2021, en fonction du nombre d'attaques.

RANG	MARCHÉ VERTICAL	FRÉQUENCE	ATTAQUE MAX.	IMPACT MAX.	DURÉE MOYENNE
1	 Traitement de données, hébergement de données et services connexes	20 798	112,28 Gbps	43,39 Mpps	68,2 minutes
2	 Fournisseurs de services de télécommunications par fil	7 845	112,28 Gbps	22,58 Mpps	116,8 minutes
3	 Fournisseurs de services de télécommunications sans fil (sauf satellite)	6 644	112,28 Gbps	22,58 Mpps	123,6 minutes
4	 Fabrication d'ordinateurs électroniques	5 382	112,28 Gbps	22,58 Mpps	131,9 minutes
5	 Toutes les autres télécommunications	3 476	112,28 Gbps	22,58 Mpps	156,7 minutes
6	 Achat électronique et sociétés de vente par correspondance	2 852	112,28 Gbps	22,58 Mpps	152,8 minutes
7	 Concessionnaires de voitures neuves	1 935	78,20 Gbps	15,81 Mpps	141,3 minutes
8	 Services de programmation informatique personnalisée	631	112,28 Gbps	22,58 Mpps	171,4 minutes
9	 Services de conseils marketing	311	5,46 Gbps	0,69 Mpps	40,0 minutes
10	 Éditeurs de logiciel	253	97,06 Gbps	18,98 Mpps	207,6 minutes

Une vue d'ensemble

Pour découvrir les toutes dernières études sur les tendances et activités dans le paysage mondial des menaces DDoS, consultez le rapport complet de NETSCOUT sur les cybermenaces (Threat Intelligence Report) pour le S1 2021.

[AFFICHER LE RAPPORT INTERACTIF](#)

NETSCOUT

© 2021 NETSCOUT SYSTEMS, INC. Tous droits réservés. NETSCOUT et le logo NETSCOUT sont des marques déposées de NETSCOUT SYSTEMS, INC., et/ou de ses filiales et/ou sociétés affiliées aux États-Unis et/ou dans d'autres pays. Tous les autres noms de produits, marques et marques de commerce, déposées ou non, sont la propriété exclusive de leurs détenteurs respectifs.

SECR_017_FR-2102 09/2021