WICHTIGE KENNZAHLEN DES NETSCOUT THREAT INTELLIGENCE-BERICHTS ZUM ERSTEN HALBJAHR 2021

DEUTSCHLAND

Der massive Online-Trend durch die COVID-19-Pandemie hat bei Cyberangreifern zu rekordverdächtigen Innovationen geführt, und das ATLAS Security Engineering & Response Team (ASERT) von NETSCOUT rechnet damit, dass diese lange Innovationsphase der Angreifer im Jahr 2021 kaum nachlassen wird.

Die Angreifer haben im ersten Halbjahr 2021 etwa 5,4 Millionen DDoS-Angriffe durchgeführt – ein weiterer Rekord. Insbesondere im ersten Quartal verzeichneten wir eine beispiellose Anzahl an DDoS-Angriffen, und die Angriffshäufigkeit nahm im Vergleich zum gleichen Zeitraum im Vorjahr um 20 Prozent zu. Gleichzeitig haben die Angreifer sieben UDP-Reflektions- und -Verstärkungsvektoren für DDoS-Angriffe entdeckt bzw. ausgenutzt und adaptive Multivektor-Angriffe entwickelt, um Schwachstellen ihrer Opfer gezielt auszunutzen. Wichtige Komponenten der Lieferkette wurden verstärkt angegriffen, während Ransomware-Gangs DDoS-Taktiken mit dreifachen Lösegeldforderungen in ihr Repertoire aufgenommen und die Fancy Lazarus-Angreifer eine neue DDoS-Erpressungskampagne gestartet haben.

Max. Multivektor-Angriff

Max. Anzahl von Vektoren in einem einzelnen Angriff

31

EINGESETZTE ANGRIFFSVEKTOREN

1. Chargen-Verstärkung
2. Citrix-ICA-Verstärkung
3. CLDAP-Verstärkung
4. COAP-Verstärkung
5. DNS
6. DNS-Verstärkung
7. ICMP
8. IMPI-Verstärkung
9. IPv4-Protokoll 0
10. ISAKMP
11. L2TP-Verstärkung
12. mDNS-Verstärkung
13. Memcached-Verstärkung
14. MSSQLRS-Verstärkung
15. NetBIOS-Verstärkung
16. NTP-Verstärkung
17. OpenVPN-Verstärkung
18. Plex-Verstärkung
19. RIPv1-Verstärkung
20. rcpbind-Verstärkung
21. SNMP-Verstärkung
22. SSDP-Verstärkung
23. STUN-Verstärkung
24. TCP ACK
25. TCP NULL
26. TCP RST
27. TCP SYN
28. TCP SYN/ACK-Verstärkung
29. Ubiquiti-Verstärkung
30. VSE-Verstärkung
31. WS-DD-Verstärkung

TOP 5-Angriffsvektoren

Ta	Dn	Ts	Im	Tr
TCP ACK	DNS-Verst.	TCP SYN	ICMP	TCP RST
ANZAHL DER ANGRIFFE	ANZAHL DER ANGRIFFE	ANZAHL DER ANGRIFFE	ANZAHL DER ANGRIFFE	ANZAHL DER ANGRIFFE
86.341	39.547	38.083	31.839	26.938

DDoS-Statistiken

Angriffshäufigkeit	-4 %
Max. Durchsatz	+27 %
Durchschnittliche Dauer	-3 %
Max. Angriffsgröße	-19 %

Größter Angriff

Größe	471,97 Gbit/s
Geschwindigkeit	270,50 MPPS
Dauer	6.982 Sekunden

Max. Spitzendurchsatz

Datum	1.2.2021
Max. Durchsatz	285 MPPS

Max. Spitzenbandbreite

Datum	1.6.2021
Max. Bandbreite	1,265 Tbit/s

NETSCOUT

Top 10 der von Angriffen betroffenen Branchen

Die folgende Tabelle zeigt eine Auswahl der im ersten Halbjahr 2021 am stärksten betroffenen Branchen nach Anzahl der Angriffe.

RANG	BRANCHE	HÄUFIGKEIT	MAX. BANDBREITE	MAX. DURCHSATZ	DURCHSCHNITTLICHE DAUER
1	**Datenverarbeitung, Hosting und ähnliche Services**	25.895	114,42 Gbit/s	27,86 MPPS	50,3 Minuten
2	**Elektronisches Einkaufen + Versandhäuser**	15.736	114,42 Gbit/s	25,67 MPPS	32,1 Minuten
3	**Drahtgebundene Telekommunikationsnetze**	6.468	114,42 Gbit/s	25,67 MPPS	57,4 Minuten
4	**Sonstige Telekommunikation**	3.306	114,42 Gbit/s	25,67 MPPS	68,9 Minuten
5	**Drahtlose Telekommunikationsanbieter (Ausnahme: Satelliten)**	2.917	112,28 Gbit/s	22,58 MPPS	47,8 Minuten
6	**Hersteller von Computern und Elektronikprodukten**	1.680	74,58 Gbit/s	16,41 MPPS	99,5 Minuten
7	**Hersteller von Speicherlösungen für Computer**	687	74,88 Gbit/s	15,88 MPPS	115,0 Minuten
8	**Internet Publishing, Rundfunk + Internetsuchportale**	622	81,86 Gbit/s	87,52 MPPS	98,5 Minuten
9	**Sonstige Pflege- und Betreuungseinrichtungen**	618	19,28 Gbit/s	2,55 MPPS	18,8 Minuten
10	**Zahnarztpraxen**	392	22,65 Gbit/s	6,64 MPPS	37,8 Minuten

Umfassende Informationen

Im ausführlichen NETSCOUT Threat Intelligence-Bericht zum ersten Halbjahr 2021 erfahren Sie mehr über den aktuellen Stand der Forschung zu Trends und Aktivitäten hinsichtlich globaler DDoS-Bedrohungen.

INTERAKTIVEN BERICHT ANZEIGEN

NETSCOUT

SECR_019_DE-2102 09/2021