2021 年上半年 NETSCOUT 威胁智能报告中的关键指标

台湾

由 COVID-19 疫情引发的向网络生活的大规模转变，促使威胁者的创新达到了破纪录的水平，而 NETSCOUT 的 ATLAS 安全工程和响应小组 (ASERT) 预计，这种攻击者创新的长尾效应将持续到 2021 年。

破坏分子在 2021 年上半年发起了大约 540 万次 DDoS 攻击，这又是一个破纪录的数字。特别是，攻击者在第一季度发起了数量空前的 DDoS 攻击，比 2020 年同期的攻击频率提升了 20%。同时，攻击者发现了七个 UDP 反射/放大的 DDoS 攻击向量或将其武器化，并开发了专门用于利用目标漏洞的适应性多向量攻击。联网供应链的重要组成部分受到越来越多的攻击，而勒索软件团伙在其武器库中增加了三重勒索的 DDoS 策略，Fancy Lazarus 威胁攻击者发起了新的 DDoS 勒索活动。

DDoS 统计数据

攻击频率	+101%
最大通量	+216%
平均持续时间	+125%
最大攻击规模	+88%

最高多向量攻击

单次攻击中看到的最大向量数 **20**

使用的攻击向量

1. Chargen 放大
2. DNS
3. DNS 放大
4. ICMP
5. ISAKMP
6. L2TP 放大
7. MDNS 放大
8. Memcached 放大
9. MSSQLRS 放大
10. NetBIOS 放大
11. NTP 放大
12. OpenVPN 放大
13. rpcbind 放大
14. SNMP 放大
15. SSDP 放大
16. STUN 放大
17. TCP ACK
18. TCP RST
19. TCP SYN
20. TCP SYN/ACK 放大

最大攻击

规模	191.04 Gbps
速度	90.38 Mpps
持续时间	2,264 秒

最大峰值通量

日期	2021/01/01
最大通量	273 Mpps

最大峰值带宽

日期	2021/05/01
最大带宽	407 Gbps

前 5 大攻击向量

Ta	Ts	Tr	Tk	Im
TCP ACK	TCP SYN	TCP RST	TCP SYN/ACK	ICMP
攻击数量	攻击数量	攻击数量	攻击数量	攻击数量
13,658	13,511	13,225	11,268	9,979

NETSCOUT

遭到攻击的十大垂直行业

下图显示了 2021 年上半年按攻击数量划分的遭到攻击最多的行业部门样本。

排名	垂直行业	频率	最大攻击	最大影响	平均持续时间
1	有线电信运营商	3,185	100.29 Gbps	87.72 Mpps	53.6 分钟
2	互联网出版、广播 + 网络搜索门户网站	695	90.18 Gbps	7.94 Mpps	57.7 分钟
3	计算机培训	174	6.11 Gbps	2.29 Mpps	35.0 分钟
4	半导体 + 相关设备制造	151	25.99 Gbps	5.95 Mpps	65.7 分钟
5	所有其他电信	100	64.82 Gbps	16.11 Mpps	34.4 分钟
6	数据处理、托管 + 相关服务	93	166.93 Gbps	20.86 Mpps	36.8 分钟
7	轮胎经销商	43	5.69 Gbps	1.17 Mpps	18.3 分钟
8	无线电信运营商（卫星除外）	37	0.84 Gbps	0.12 Mpps	12.8 分钟
9	电子计算机制造	36	1.34 Gbps	0.17 Mpps	70.2 分钟
10	所有其他专业、科学 + 技术服务	2	0.31 Gbps	0.05 Mpps	12.0 分钟

整体情况

探索 2021 年上半年 NETSCOUT 威胁智能报告全文，了解对全球 DDoS 威胁领域的趋势和活动的最新研究。

查看交互式报告

NETSCOUT

SECR_039_ZH-2102 09/2021