2020 DDoS攻击现状与趋势调查

威睿DDoS安全防御团队

2020
DDoS攻击现状与
趋势统计报告

前言

随着网络科技的兴起与普及，分散式阻断服务攻击(Distributed Denial of Service, DDoS)的规模与次数与日具增，持续以更创新、复杂的攻击手法，对企业组织带来莫大的威胁。企业网络一旦因DDoS攻击导致服务中断或停机，除了营运受影响、机密资料外泄等问题外，也可能遭受骇客勒索赎金，让公司面临庞大的潜在损失。

混乱的2020年，更由于COVID-19全球性疫情的推波助澜，顺势带动了宅经济、在家办公、远距教学等网络活动的迅速发展，但也因此成为网络骇客发动攻击的绝佳契机，让DDoS攻击次数及规模达到前所未有的高峰。防堵DDoS攻击不再是新话题，却已经是任何企业组织都不可忽视的资安议题。

身为亚太区网络流量分析与DDoS安全的领导厂商，威睿科技(Genie Networks)持续专注于电信及网络运营商市场。有别于一般企业网络，这些电信等级的网络规模不仅更大，架构也更为复杂，因此需要高于一般市场规格与性能的检测防御系统以保障其安全性。威睿科技的DDoS防护解决方案，专门对应这些客户的资安需求，在过去的20余年，我们已成功协助全球数百家电信及网络运营商免于DDoS攻击的威胁。

这份年度调查报告，由威睿科技针对2020年的DDoS攻击活动进行观测及统计，调查对象为亚太区数个大型电信及网络运营商(Internet Service Provider)网络，其服务类型包含：网际网络接取服务(Internet connection services) 、资料中心/云中心/主机代管中心(Data center/co-location services)、以及行动数据服务(Mobile data network infrastructure)。

本调查报告以威睿科技的流量分析及DDoS侦测产品 – GenieATM所收集的数据资料进行分析，由于GenieATM主要针对网络第3、第4层的巨量型(Volumetric)DDoS攻击检测，因此本报告也将专注于呈现巨量型DDoS攻击的相关统计数据。除了攻击方式的类型分布、趋势、规模、时长、来源分布等进行量化的统计外，也会分享2020年前几个规模最大的巨量攻击案例剖析。

有别于市面上普遍的DDoS攻击统计报告，其内容多半仰赖对调查对象的主观式问卷调查，本调查报告采用现网的实际攻击统计数据进行分析，使其呈现的资讯不受主观记忆和观点影响，尽可能提供最真实客观的统计分析报告。

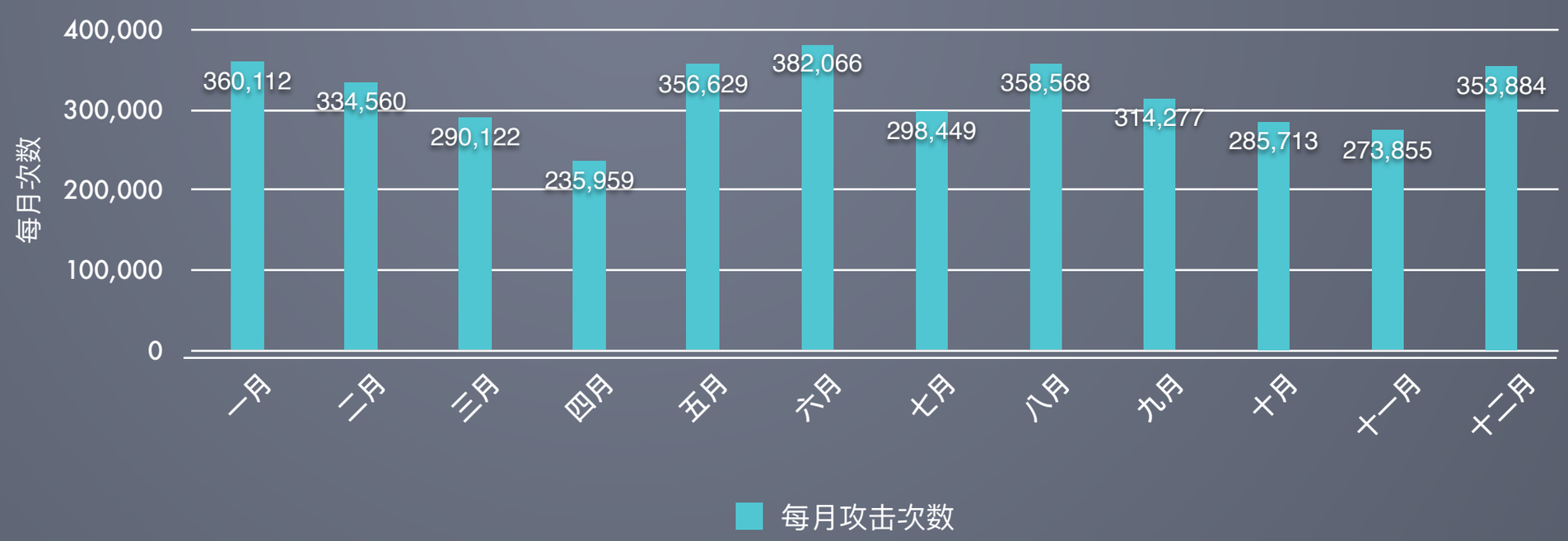
威睿DDoS安全防御团队

2020
DDoS攻击现状与
趋势统计报告

攻击频率趋势

观察2020年检测到的DDoS攻击事件频率，全年总计约370万次。每个月观测的攻击事件，约略在20万到40万次之间，以6月份到达最高峰的38万多次，以4月份的次数最少为23万多次。逐月攻击频率有相当程度的波动，每月成长/衰退幅度(MoM+)约在-15%～+40%之间，平均每月约有30万次的攻击。相当于：

- ✓ 每日 10,146次；
- ✓ 每小时有 423次；
- ✓ 每分钟就有 7次攻击发生。



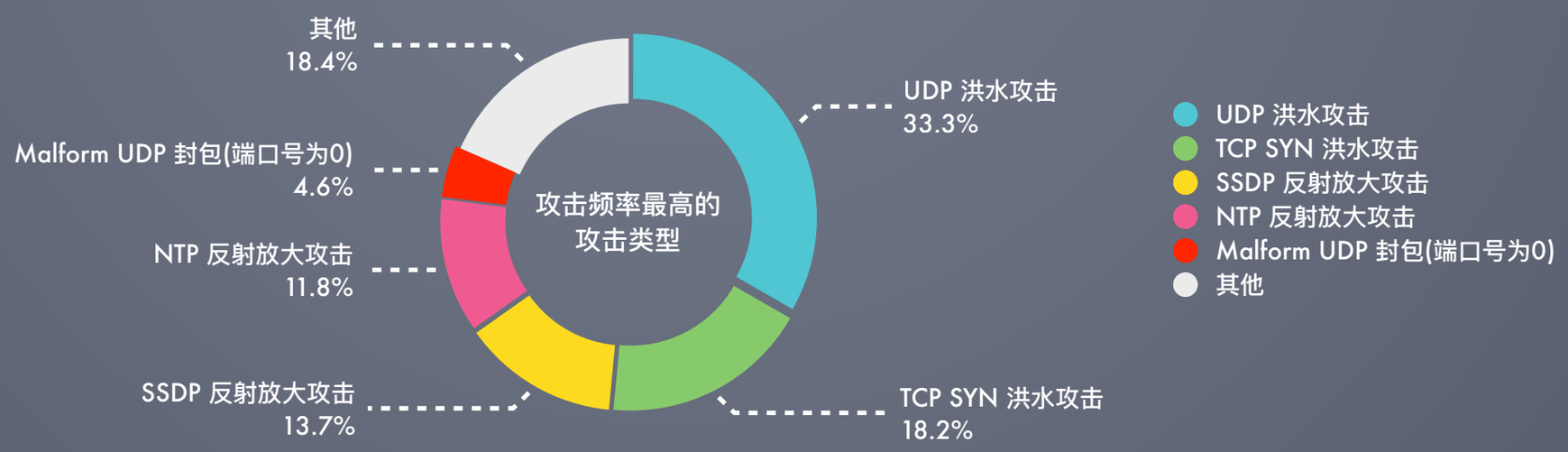
攻击频率 | 攻击类型(ATTACK VECTOR)占比

在此次观察报告中，我们统计数十种的DDoS攻击类型(Attack Vector)，而这些攻击主要又可分为几大类别：TCP洪水攻击 (如SYN Flooding, RST Flooding, SYN-RST Flooding……等)、 UDP洪水攻击、协议滥用攻击 (如Malformed TCP封包、Malformed UDP封包、Land Attack, IP Protocol Null, ICMP滥用……等)、反射放大攻击 (如SSDP Amplification, NTP Amplification, CLDAP Amplification, DNS Amplification……等)、 蠕虫攻击 (如SQL Slammer, Code Red, Sasser……等)、应用层洪水攻击等等。

观察统计2020年的DDoS攻击事件频率，前五大常出现的攻击类型分别为：

- ✓ 1st, UDP洪水攻击, 占约总次数的33.3%
- ✓ 2nd, TCP SYN洪水攻击, 占约总次数的18.2%
- ✓ 3rd, SSDP反射放大攻击, 占约总次数的13.7%
- ✓ 4th, NTP反射放大攻击, 占约总次数的11.8%
- ✓ 5th, Malformed UDP封包 (端口号为0), 占约总次数的4.6%
- ✓ 其他类型攻击次数合计，约占总次数的18.4%

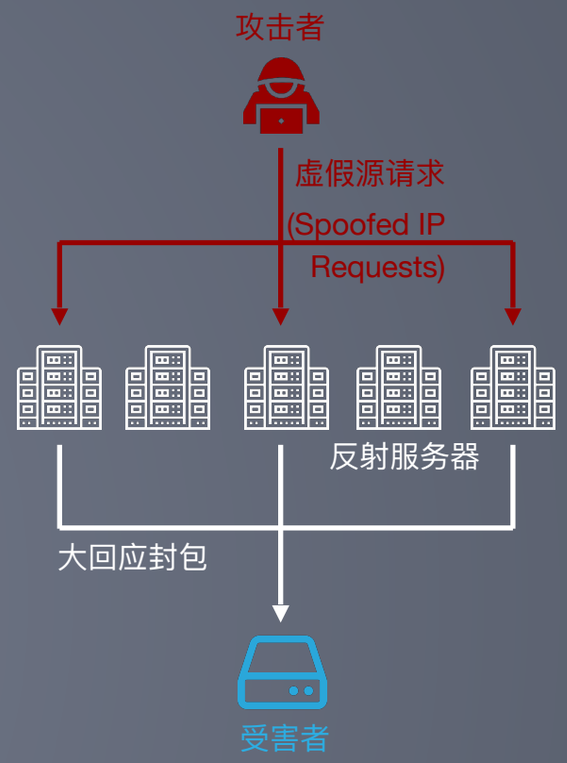
若以大类别归纳，2020年最主要的攻击型态为反射放大攻击，其次为UDP及TCP SYN洪水攻击。

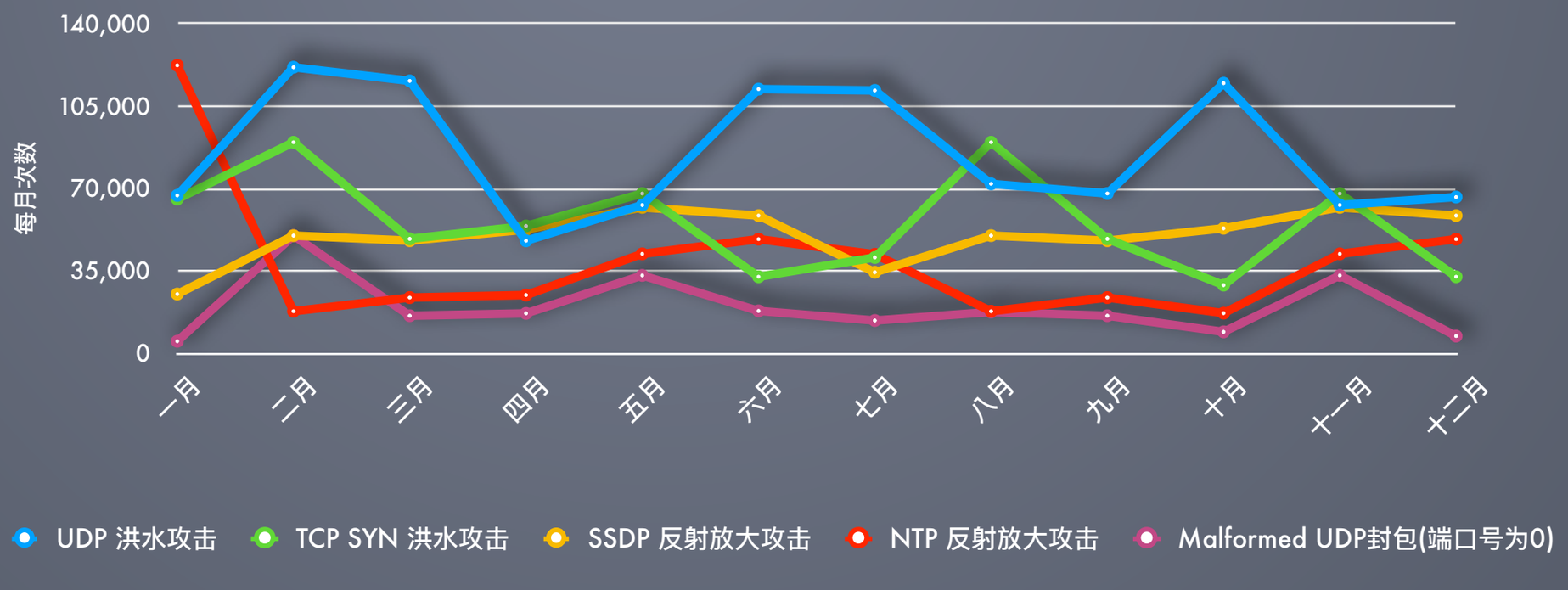


攻击频率 | 攻击类型(ATTACK VECTOR)趋势

2020年的逐月Top5攻击类型没有太大变动，大致上都是UDP洪水攻击、TCP洪水攻击、SSDP反射放大攻击、NTP反射放大攻击及 Malformed UDP封包攻击分占前5名，除了在少数月份有TCP RST洪水攻击及DNS反射放大攻击挤进前5名，以及1月时DNS反射放大攻击挤进第5名之外。

此外，排名第5的Malformed UDP 封包(端口号为0)攻击流量的形成，经观察分析发现，主要是反射放大攻击的伴随效应。因为在反射放大攻击如SSDP、NTP等反射放大攻击的攻击过程中，通常会使得反射服务器以极大的UDP封包回应攻击者的虚假请求 (Spoofed IP Requests)，而这些被利用作为反射放大攻击的反射服务器通常会回应以放大倍率(Amplification Factor)极高的大封包。而过大的UDP封包在传送时需要被切段(Fragmentation)成较小的IP封包传送，使得除了首个IP封包片段(fragment)带有UDP封包标头(header)的完整的资讯外，其他后续的IP片段封包则会被路由器视为没有UDP封包标头，造成后续IP片段封包被路由器等识别统计为UDP源/目的端口号均为0的通讯协定异常封包。所以，Malformed UDP封包攻击流量常高踞第5名，是反映出主要攻击型态为反射放大攻击的现况。



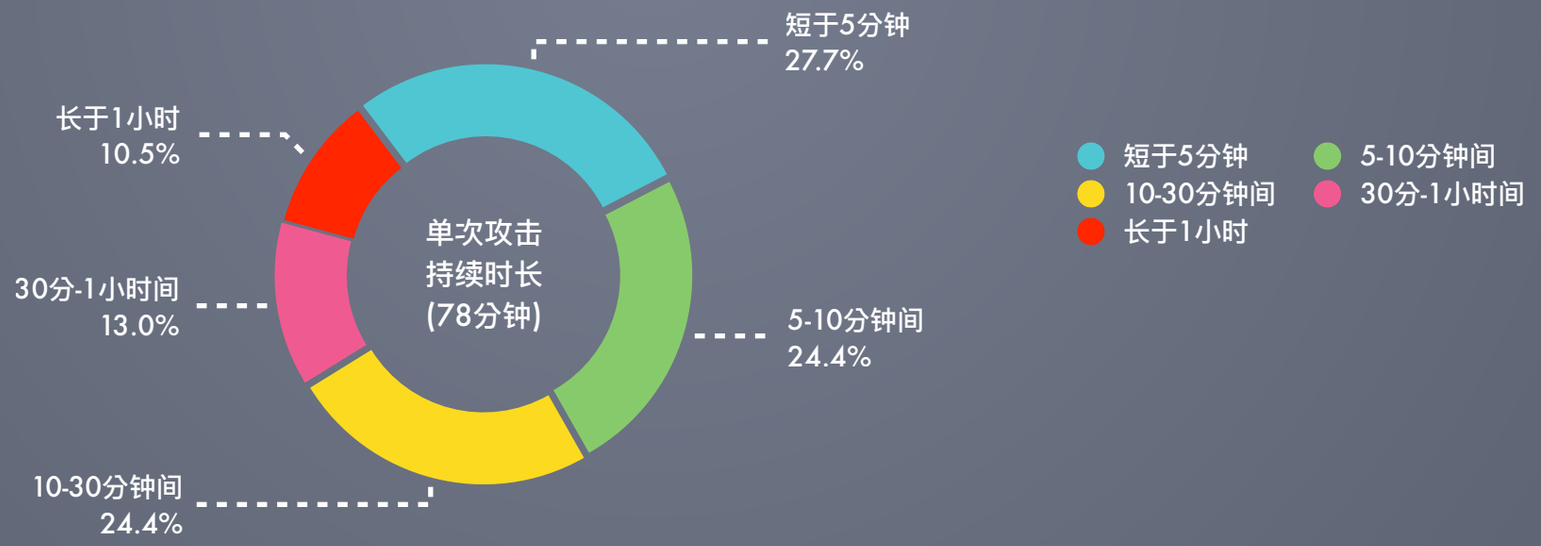


攻击频率 | 攻击时长分布

统计2020年观测到的DDoS攻击事件，每次攻击的持续时间平均约 78分钟(1.3小时)，而大多数的攻击常在5分钟内结束。

我们观察到将近半数的攻击事件持续时间都在5到30分钟之间，约有28%的攻击事件持续时间则短于5分钟，而长于1小时的攻击仅占全部事件的11%，然而总平均攻击时长却长达一个小时。这是因为虽然长于1小时的攻击次数仅占少数，但其持续时间往往不只是1个多小时，部份攻击甚至持续了数十小时、数日的时间，因此在统计上会大幅拉高整体时长的平均值。

此外，极大比例的攻击由出现、产生大规模流量、到攻击流量结束，时间持续不过短短数分钟。因此能否在流量巨增之初，就能以最快的时间检测、告警及处理，将会是对巨量DDoS攻击防御的重要关键之一。

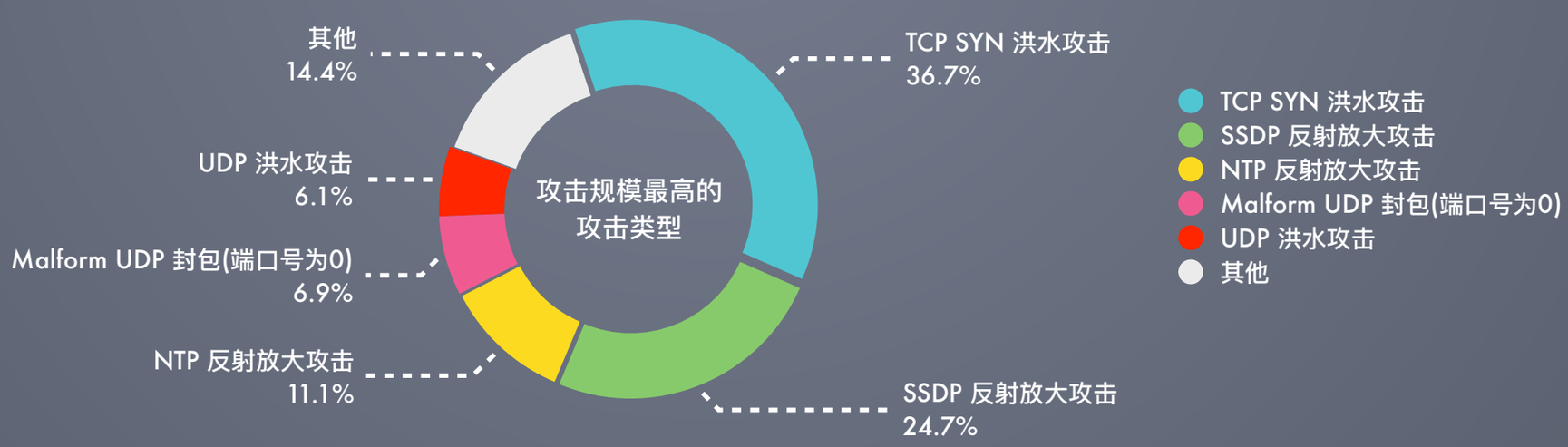


攻击规模 | 攻击类型(ATTACK VECTOR)分布

2020年观测到的DDoS攻击事件，以攻击流量的规模计算，前五大攻击类型分别为：

- ✓ 1st, TCP SYN洪水攻击, 占约总攻击流量的36.7%
- ✓ 2nd, SSDP反射放大攻击, 占约总攻击流量的24.7%
- ✓ 3rd, NTP反射放大攻击, 占约总攻击流量的11.1%
- ✓ 4th, Malformed UDP封包(端口号为0), 占约总攻击流量的6.9%
- ✓ 5th, UDP洪水攻击, 占约总攻击流量的6.1%
- ✓ 其他类型攻击流量总合，约占总攻击流量14.4%

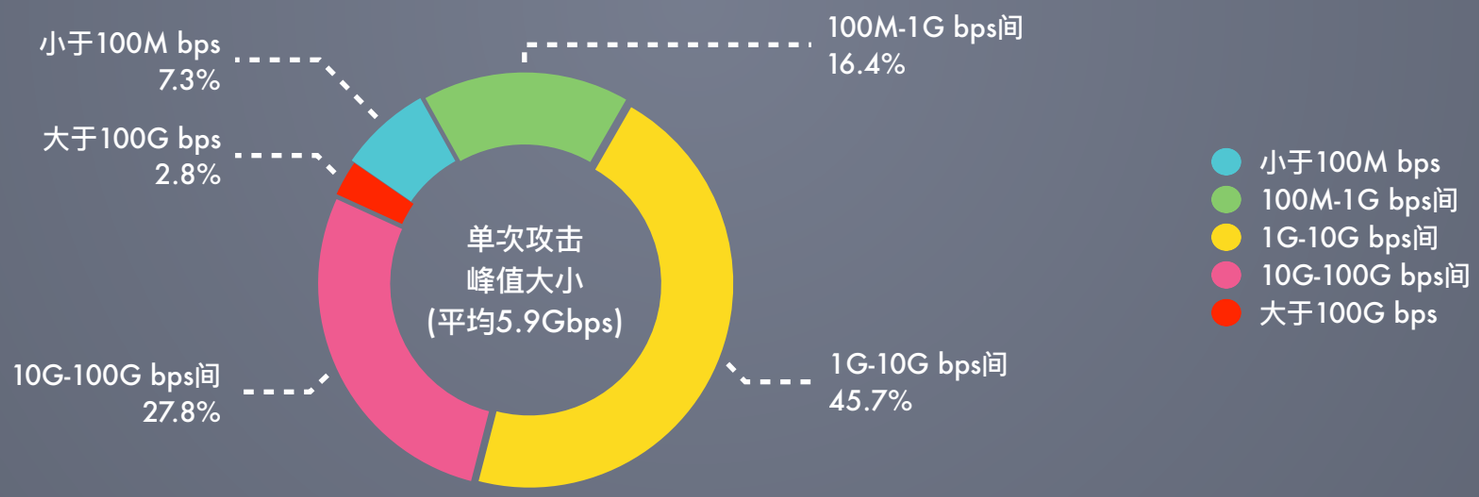
将攻击流量规模占比Top 5 和 攻击频率占比Top 5 两相对照比较，可以发现：UDP洪水攻击的单次攻击规模，相较于反射放大攻击或TCP SYN洪水攻击等，一般而言单次攻击规模较小，因而使得前 5 大的攻击虽然类型不变，但以攻击流量规模论，排名上UDP洪水攻击的排名由频率最高的第一名降到第五名。



攻击规模 | 攻击大小分布

统计2020年观测到的DDoS攻击事件，单次攻击的平均峰值大小约5.5G bps，单次攻击峰值大小最多落在1Gbps到10Gbps间。

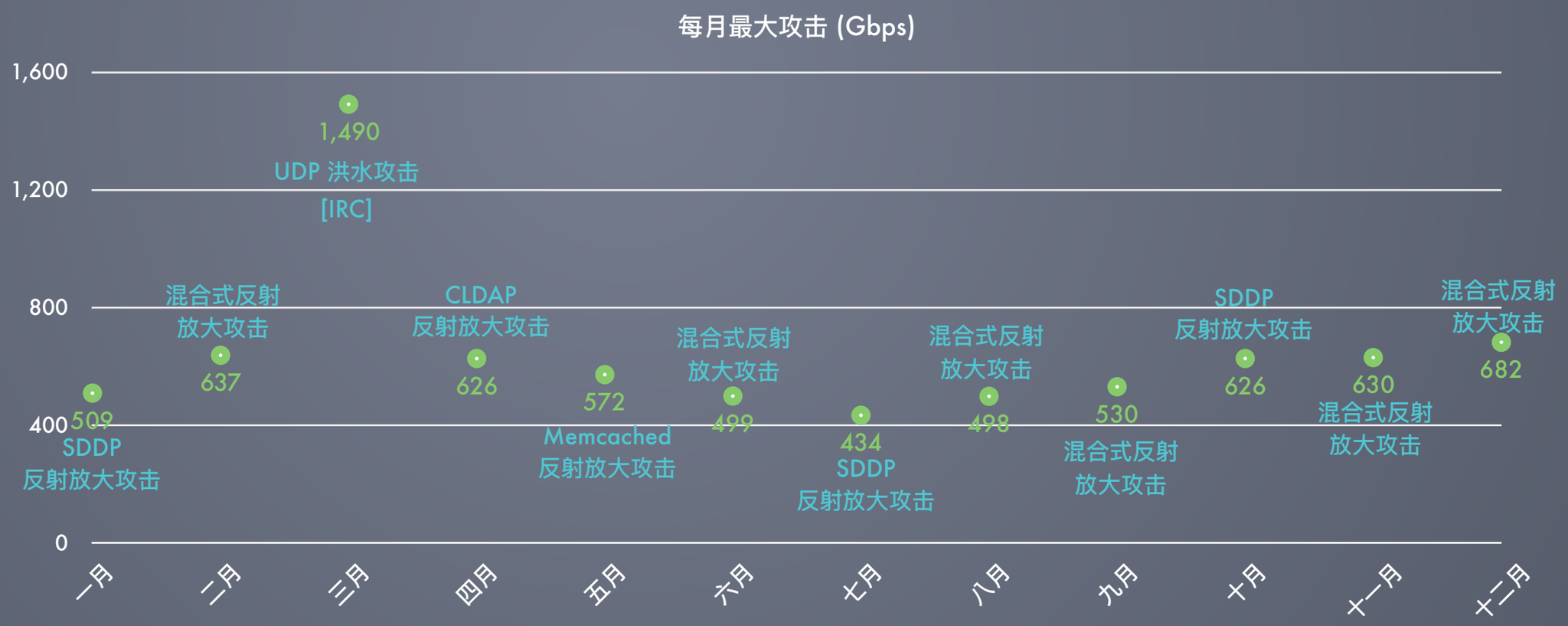
进一步分析不同攻击类型的单次攻击规模，发现不同攻击类型单次攻击峰值平均规模差异极大。单次攻击峰值平均规模较大的攻击类型有反射放大攻击、TCP SYN 洪水攻击、Malformed TCP 或UDP封包攻击等，其单次攻击平均规模都高达20Gbps以上；而单次攻击峰值平均规模较小的攻击类型则有像蠕虫攻击及特定协议误用攻击等，其单次攻击一般在数百Mbps的规模。故可以发现因类型的不同，一般大规模的攻击类型和一般小规模的攻击，其攻击平均规模大小可达数百倍。



巨量攻击 | 逐月巨量攻击趋势

以每个月为单位，我们记录了每月的最大攻击规模及其类型。由下图表可见，2020全年每月检测到的最大攻击，除了三月间发生的最大攻击事件，其攻击流量规模高达1.49T bps外，每月最大攻击的规模一般落于 400G bps至700G bps之间。

此外，观察发现巨量攻击类型主要多为反射放大式攻击、或由反射放大攻击组合而成的混合式攻击(Multi-vector attack)。唯独在三月检测到的攻击为一个锁定特定目的地端口号的UDP洪水攻击。接下来，我们将进一步剖析数个2020年巨量规模攻击的流量特性。

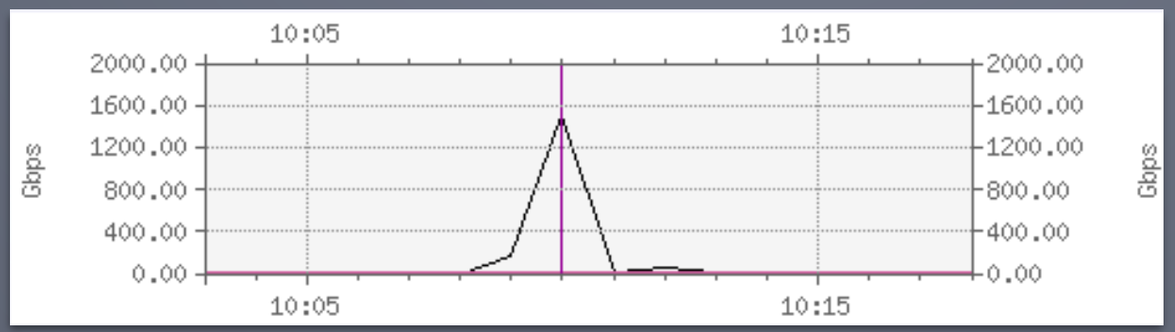


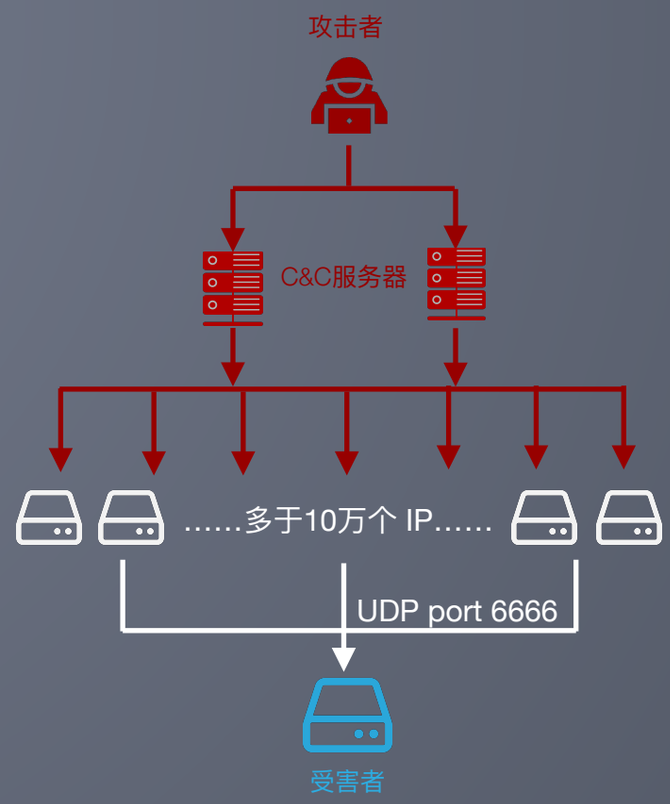
巨量攻击 | 案例分析 1

2020年检测到的最大攻击，发生在3月22日上午10时08分，攻击峰值高达1,490G bps，攻击持续仅5分钟26秒。该攻击是一个来源位址极分散的大规模UDP洪水攻击，由超过10个路由器灌入受害网络，在两分钟内攻击流量就暴冲到近1.5T bps的峰值。在攻击达峰值时，评估约有超过10万个攻击IP位址同时发送大小约 408 Bytes的封包，到受害主机的UDP端口号6666。受害主机为一云服务中心的服务器，而这些攻击流量的源位址都来自于亚太国内。

进一步探讨这个攻击的流量行为：它使用的UDP端口号6666一般被用于Internet Relay Chat (IRC)通讯。IRC协定通常被用于在主从式架构(client-server model)下传送文本(text)形式的资料，目前已知UDP端口号6666常是Kali Linux木马工具使用的通讯端口号之一。在这次的巨量攻击中，单一受害主机受到超过10万个源IP以高于3.6G pps的速度发送流量封包，是一次规模极为可观的殭尸网络(Botnet)攻击。

所谓的殭尸网络是由许多受到恶意程式感染的连网设备所组成，骇客常利用这些因感染而可以远端控制的装置来发动大规模攻击，而殭尸网络的威力主要由受感染设备的数量规模来决定。过往要实现一个DDoS攻击并不容易，但随着物联网(IoT)的问世，促使联网的装置数量大幅度增长，再加上物联网设备普遍资安标准较为松散的特性，正好让殭尸网络骇客找到了征服大量设备的新宝地。以3月发生的这个巨量攻击为例，同一时间能发动数万个源IP进行攻击，创下每秒Tb级的攻击流量，正符合IoT殭尸网络的攻击场景。



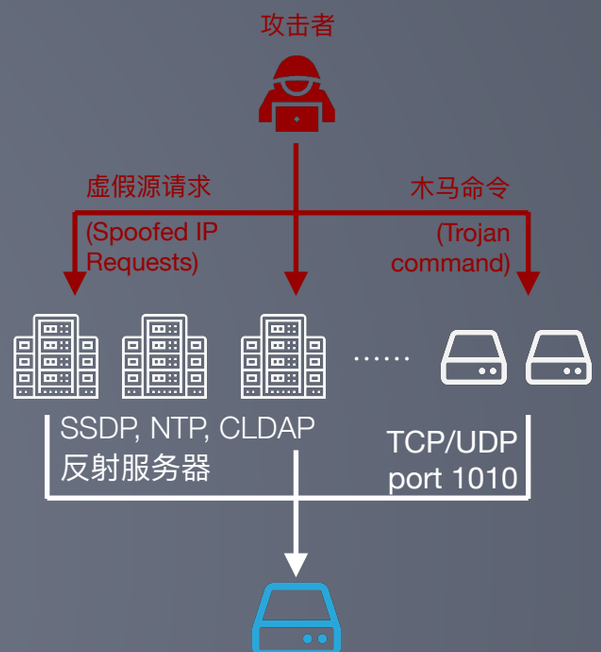


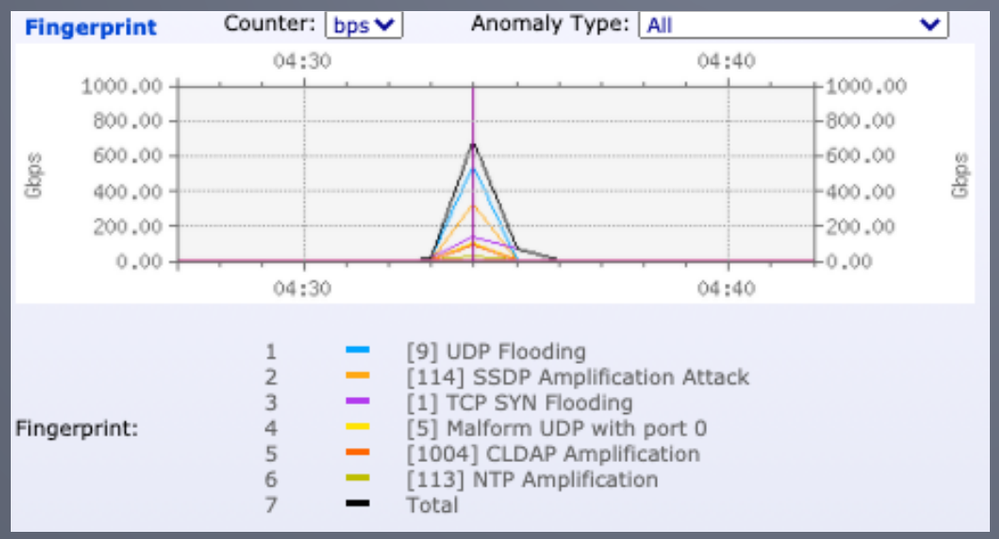
巨量攻击 | 案例分析 2

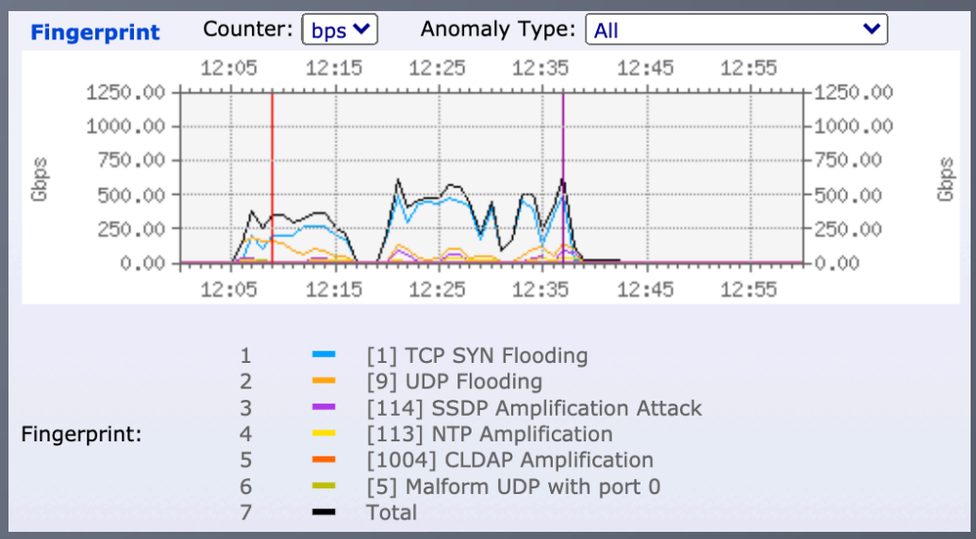
除了一次高达将近1.5Tbps的巨量攻击外，2020年次大及第三大攻击均为大规模的混合型攻击，分别发生在年末的12月3日凌晨4时和年初的2月12日上午10时，攻击峰值各高达682G bps及637G bps。在攻击时长上，则一短一长，一个仅持续约5分钟，而另一巨量攻击则持续了约42分钟之久。

这两个巨量攻击型态，都属于大规模的混合型攻击攻击。攻击结合了数种常见的反射放大攻击，包含有SSDP反射放大攻击、NTP反射放大攻击、CLDAP反射放大攻击和反射放大攻击伴随的Malformed UDP封包流量等等。除了反射放大攻击，这个混合攻击还包含了相当的TCP SYN洪水攻击流量，瞄准如目的地端口80， 甚或以数个高端口号源端口流量瞄准特定的TCP/UDP1010目的地端口的Doly木马程式攻击。

这样的巨量攻击在攻击流量最猛烈时，有超过数百个的攻击IP位址同时以不同的通讯协定(TCP, SSDP, NTP, CLDAP等)，经由数十个路由器链路将攻击流量，灌入受害网络。而这两个巨量攻击则分别的源自于国内它家电信业者的网络，以及来自于亚太国内外。



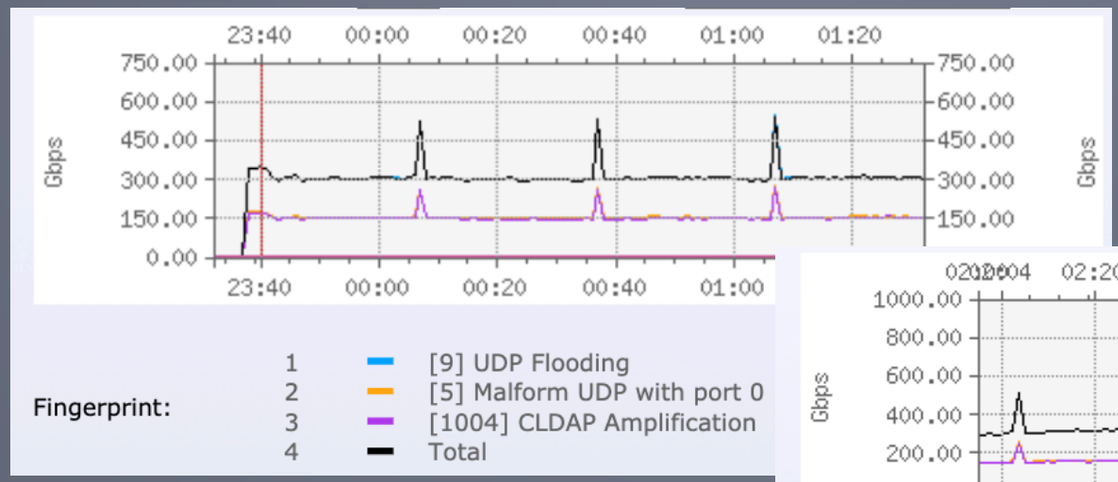


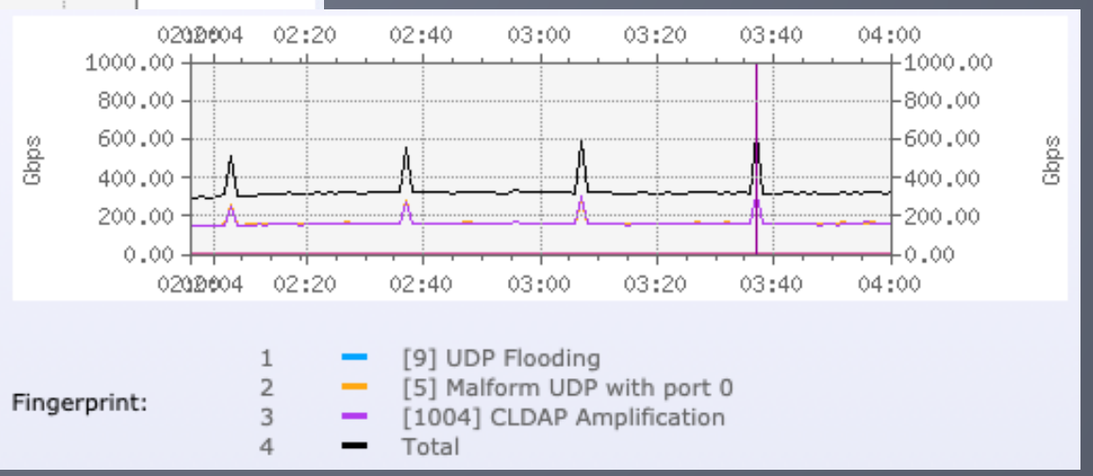


巨量攻击 | 案例分析 3

2020年检测到的第四大攻击，发生在今年4月18日晚间23时37分，攻击峰值达626G bps。该攻击是一个大规模的CLDAP反射放大攻击，伴随着大量的Malformed UDP封包流量。这次攻击在异常流量出现半小时后流量达到短暂的峰值，在攻击达峰值时，评估约有超过上千个反射攻击伺服同时以CLDAP通讯协定攻击受害主机。

这个巨量攻击和前述几个巨量攻击相比，另有三大特别之处：首先，它攻击源的反射攻击服务器主要多来自于国外运营商，如Microsoft、Amazon、瑞典、南非等等；第二，它的攻击时长持续了3天又11小时多后，流量才回归一般正常水准；第三，这个反射放大攻击流量并非持续地处于流量高原，而是一种规律出现流量突刺的脉冲波型攻击(Pulse Wave attack)。在这次巨量攻击中，我们可观察到固定每隔半小时就会出现流量突刺，流量的突刺峰值高达600多Gbps。这样的流量突刺模式持续了约三天，突刺流量值逐渐衰减，最终归于无突刺的流量高原，并于三天后流量值恢复正常。





结语

观察2020年的DDoS攻击活动，以攻击事件频率而言，巨量型DDoS攻击在2020年共有多达370万次，平均每月多达30万次，其中最大的攻击规模高达1.5Tbps，最长的攻击甚至持续了三日之久。以单一攻击类型的频率来看，UDP洪水攻击高居榜首，占总频率的3成之多，以大类别的攻击频率计算，最常出现的类型为反射放大攻击，若以攻击规模而言，则是TCP SYN洪水攻击占最多数。统计2020整年度发生的DDoS攻击事件，平均攻击峰值的大小大多落在1～10Gbps之间，而大于100Gbps规模的巨量攻击次数也有高达10万多次。 以攻击时长来看，将近半数的攻击事件持续时间均落在5到30分钟之间，多数攻击甚至持续不到5分钟，而长于1小时的攻击仅占10.5%。

进一步观察每月规模具代表性的巨量DDoS攻击，发现混合型攻击为巨量攻击的主流，通常由数种反射放大攻击甚或TCP/UDP洪水攻击所组合而成。我们也在报告中分享了2020年的前几大巨量攻击案例，其攻击类型包含：由物联网装置驱动的殭尸网络攻击；结合反射放大攻击与洪水攻击的混合型攻击；以及规律、持续性的脉冲波攻击。

由这份观察报告不难发现，DDoS攻击手法越变越多元复杂，攻击力度越来越猛烈的趋势，这都会使传统防御解决方案遭受到严峻的挑战。一个有效对应的解决方案，必须在防御技术上与时具进，提供趋近即时的回应速度、异常流量行为聚合、以及完善的检测判定机制。

展望未来，疫情终究会结束，但物联网等高速网络应用的发展已成为全球大势，我们认为，DDoS攻击将持续是各大电信网络运营商的重大资安威胁。期待这份DDoS现况与趋势观察报告，除了能让电信网络运营商进一步了解网络攻击的整体趋势与攻击属性，做为制定网络安全政策及防御工作部署的参考外，也期许对复杂攻击流量行为的深入探察，也能做为评估、乃至于开发DDoS防御解决方案时的一项重要依据，做为机器学习、AI智能化检测等新型防御技术研究应用的背景资讯。身为电信网络运营商最信赖的DDoS安全伙伴，威睿科技将持续以更贴近市场的产品线及分析研究报告，提供更完善的资安解决方案与专业洞见。

欢迎对本报告内容提出您宝贵的批评指教，请将您的反馈意见邮寄至：sales@genie-network.com