中国云服务商网络风险报告

2018 年

安全值

二〇一八年九月

目录

第 1 章 概述 1
1.1 云服务商安全的概述 1
1.2 名词解释 1
第 2 章 云服务商安全矩阵 3
2.1 安全风险值概况 3
2.2 云服务商四维评价 3
2.3 云服务商资产 R-S 风险相关关系分析 4
2.4 云服务商流行度 P-R 风险相关关系分析 6
第 3 章 云服务商网络风险分析 7
3.1 云服务商网络风险概况 7
第 4 章 云服务商安全漏洞分析 9
4.1 云服务商最常见安全漏洞分析 9
4.2 安全漏洞详细统计和描述 9
4.3 SSL 高危风险 10
第 5 章 网络攻击分析 12
5.1 云服务商 DDoS 攻击概况 12
5.2 云服务商 DDoS 攻击流量年度统计情况 13
5.3 高危端口风险 13
第 6 章 其他网络风险分析 15
6.1 HTTPS 证书过期 15
第 7 章 附录 16

第1章 概述

1.1 云服务商安全的概述

随着 IT 资源服务化思想日益普及，计算资源呈现出“一切皆服务”的趋势，资源服务成为云计算的核心运营模式。然而，在云计算带来便利的同时，服务资源的集约化、虚拟化也进一步增加了安全防范的难度，云服务商的安全问题日益凸显，逐渐成为云计算技术推广落地的核心研究课题之一。

然而，全球云服务相关的安全事故却时有发生：2016 年 9 月，Cloudflare 数百万网络托管客户数据泄露；2017 年 6 月，亚马逊 AWS 公有云共和党数据库中美国 2 亿选民个人信息被曝光；近日，在腾讯云发生了一起因服务器故障，导致创业公司数据丢失的事件；数据丢失对于企业来讲将会造成不可估量的损失，在企业将业务应用向第三方云环境迁移的过程中，首先需要考虑的就是对云服务的信任问题。由于云服务的“外包”特性，云服务商是否能够对租户数据安全提供保障，能否为其业务运营保驾护航，能否采用积极手段挽回事件损失直接成为云计算厂商竞争的核心能力。云服务商层出不穷的安全事件直接把云安全推向了网络安全研究的前沿，安全值就 70 家云服务商进行网络安全风险研究，形成如下报告。

1.2 名词解释

- **安全漏洞：**主机操作系统和安装的组件存在的严重的高危漏洞，会使服务器遭受病毒或黑客入侵，引起信息泄露或篡改。
- **网络攻击：**企业在互联网上的应用系统或网络遭受到 DDOS 拒绝服务攻击，包括 TCP 攻击或 UDP 攻击的报警信息，拒绝服务攻击通过流量攻击的方式攻击系统或网络，过大的攻击流量会引起服务中断。
- **垃圾邮件：**组织邮箱服务器被列为垃圾邮件发送域，一旦被反垃圾邮件设备拦截，将导致用户可能无法正常使用邮件。
- **恶意代码：**来自国内外安全厂商的恶意代码检测结果，系统可能已经被植入后门、病毒或者恶意脚本。

- **僵尸网络：**组织服务器被攻破，被当做“肉鸡”不断向外部发起扫描或者攻击行为，服务器主机可能被入侵，存在后门被远程控制。
- **黑名单：**域名或者 IP 地址被权威黑名单机构列入黑名单，用户的正常网页访问可能被浏览器拦截或者 IP 网络通讯被防火墙阻断。
- **高危端口：**黑客会使用工具扫描计算机上的端口，并入侵这些端口，关闭这些高危端口，可使电脑避免遭受攻击。
- **证书过期：**网站证书过期，造成无法对外提供服务，影响用户访问。犯罪分子利用过期的证书，可窃取和篡改浏览器与服务器之间的信息传输。

第2章 云服务商安全矩阵

2.1 安全风险值概况

安全值对近一年内全国云服务商的互联网资产和面临的网络风险进行了重点分析，整个行业网络安全均值为 573，属于风险较高的行业。对于抽样分析网络风险的 70 家云服务商中，其中分数低于 850 分的有 54 家，处于网络风险的高危地段。云服务行业共有互联网资产 140223 个，其中域名 229 个，主机 108991 个，IP 地址 31003 个；网络风险共计 243261 个，其中包括安全漏洞 5419 个，网络攻击 11321 次，僵尸网络 226110 次，恶意代码 362 个，域名隐私泄露 49 个。

2.2 云服务商四维评价

云服务商网络风险较高的 TOP10

公司名称	风险值 R	资产规模 S	风险趋势 T	流行度 P
北京光环新网科技股份有限公司	104	10.0	1	37.9
新网数码	104	10.0	-12	33.2
京东	111	10.0	0	60.9
阿里云计算有限公司	130	10.0	-57	52.0
苏宁云商集团股份有限公司	158	8.3	2	51.9
北京金山云网络技术有限公司	226	7.8	-6	46.0
上海斐讯	227	6.9	-25	24
中兴通讯股份有限公司	228	5.6	17	32.5
甘肃万维信息技术有限责任公司	245	8.1	12	26.9
北京万国长安科技有限公司	335	3.5	-12	25.8

云服务商网络风险较低的 TOP10

公司名称	风险值 R	资产规模 S	风险趋势 T	流行度 P
山东众志	937	1.7	0	14.6
未来国际	937	2.8	0	19.4
快云	937	2.6	0	26.9
百度云	1000	1.8	0	47.2

世纪互联	1000	1.6	0	15.8
国富瑞	1000	2.2	0	12.1
阅联	1000	1.9	0	15.6
犀思云	1000	1.8	0	13.0
联想	1000	1.4	0	26.4
互联港湾	1000	2.5	0	12.6

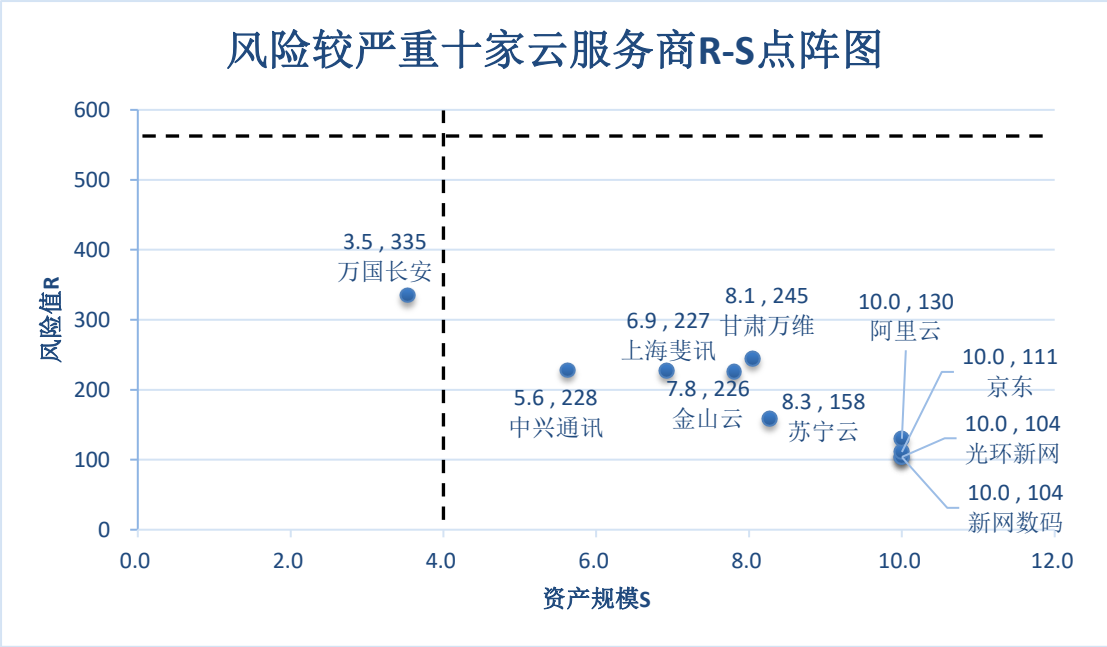
为了能够深入研究行业互联网风险状况及原因，我们选择了安全值较低和较高的各十家公司进行 RSTP 四维分析评价。分别从风险值、资产规模、风险趋势、流行度等角度的数据分析了各行业风险状况及其内在相关关系。从上表可以看出互联网资产规模较为庞大的云服务商大部分处于网络风险较高的地带，同样访问流行度高的几家云服务商均拥有着偏高的互联网资产数量。

名词解释：

- **风险值（R）：Risk，评分区间（0-1000 分），风险越高 R 值越低。**
- **资产规模（S）：Scale，评分区间（0-10 分），机构的资产数量越多 S 值越高。**
- **风险趋势（T）：Trend，评分区间（±1000 分），当月与前一月 R 值变化趋势。**
- **流行度（P）：Popular，评分区间（0-100 分），被访问次数越多 P 值越高。**

2.3 云服务商资产 R-S 风险相关关系分析

云计算企业搭建云平台时，可能会涉及购买第三方厂商的基础设备、运营商的网络服务等情况。基础设施、网络等都是决定云平台稳定运行的关键因素。云服务将资源和数据的所有权、管理权和使用权进行了分离，故云服务商需要具有更高的数据安全保护水平和更先进的数据保护手段。因而我们针对云服务商的风险值和互联网资产指数做以下分析：



为了研究资产数量和网络风险的影响，我们选取了网络风险值较低的十家，根据表中数据绘制了象限图。从图中分布可以看出抽样企业的风险值 R 随着资产规模扩大而降低，图中虚线代表了行业平均资产规模及平均风险值；我们可以发现网络风险较高的十家云供应商大部分处于第四象限，也就是资产最多的云服务商安全值最低，说明互联网资产的增加同样也扩大了风险的暴露面，为云服务带来了更多的互联网风险，云服务商应采取更加完善的信息安全工作。

我们选择了处于高危风险的十家云服务商，分析其资产详细情况。将互联网资产分为域名资产、主机资产、IP 资产、CDN 等几个维度进行统计结果如下：

云服务商互联网资产概况

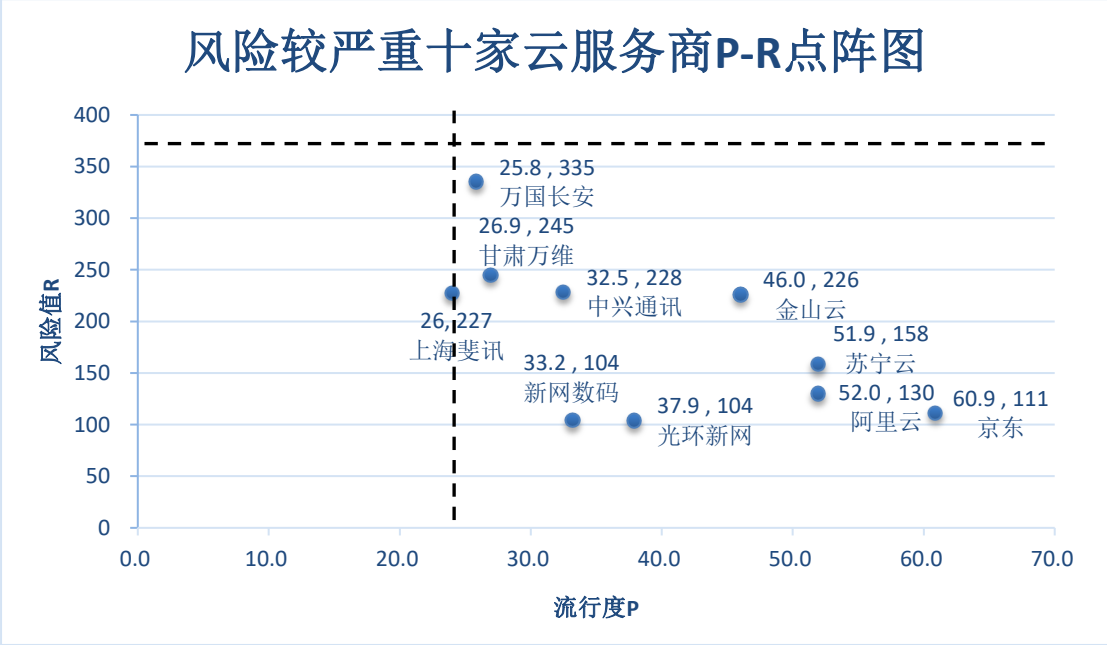
公司名称	风险值	域名数	主机数	IP 数	CDN
光环新网	104	9	16346	9566	5951
新网数码	104	15	6558	5457	21
京东	111	26	11377	3194	1263
阿里云	130	9	20109	9923	4294
苏宁云	158	33	3330	416	977
金山云	226	1	1714	198	44
上海斐讯	227	1	181	147	31
中兴	228	5	309	232	25

甘肃万维	245	32	585	80	1
万国长安	335	1	57	44	7

注：数据来源安全值，以上数据为 2017 年 7 月~2018 年 7 月存活过的互联网资产累计数值。

从表中可以看出，域名数最多的是苏宁云；主机数和 IP 数最多的均是阿里云；其中 CDN 最多的是光环新网。CDN 作为一种新型的网络构建方式，它不仅能大大提高网络站点的访问速度以及站点稳定性，还能有效地预防黑客入侵以及降低各种 DDoS 攻击对网站的影响，同时保证较好的服务质量。

2.4 云服务商流行度 P-R 风险相关关系分析



为了研究访问流行度和网络风险的关系，选取云服务商中风险值较低的十家平台，根据表中数据绘制了象限图。图中虚线代表了平均访问量及平均风险值，从整体走向可以看出，访问流行度较高的企业相对应的风险值均较低；访问流行度代表着企业云服务的访问频率及用户规范，越是活跃的组织系统重要性越高，但目前的网络安全风险却最高。

第3章 云服务商网络风险分析

3.1 云服务商网络风险概况

云服务商网络风险概况

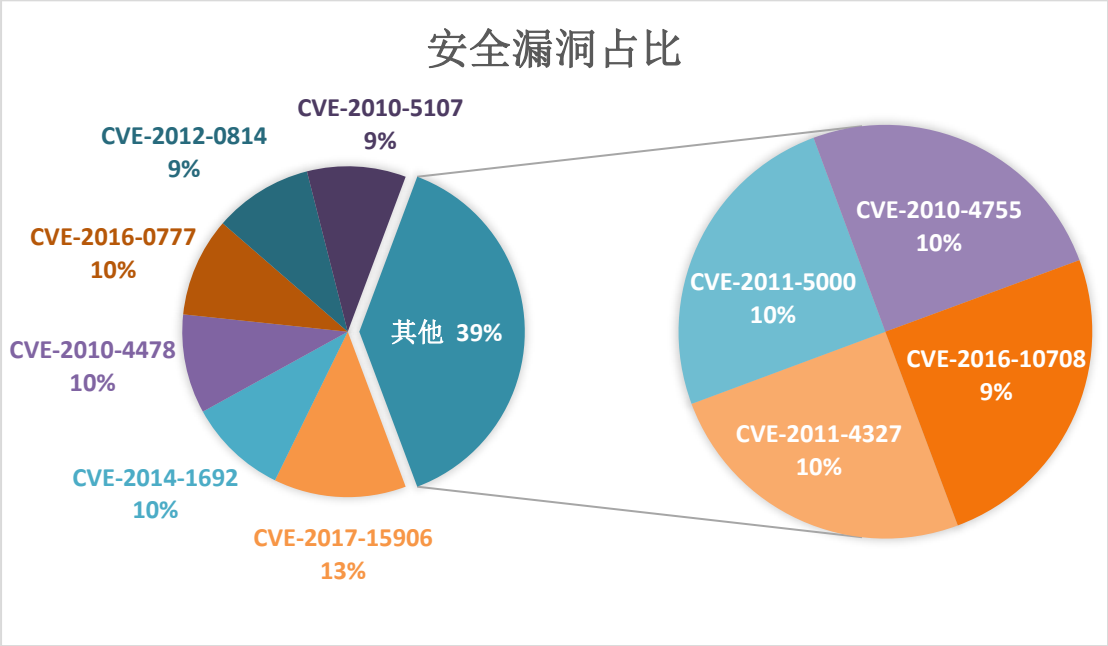
公司名称	风险值	网络攻击	安全漏洞	域名隐私是否泄漏	恶意代码	僵尸网络	IP 黑名单	端口高危风险	SSL 高危风险
光环新网	104	923	863	是	2	188633	27	35	2
新网数码	104	3162	3619	是	2	2806		681	2
京东	111	1668	194	是	2	6893	1	2	0
阿里云	130	2294	40	否	6	2755	12	0	0
苏宁云	158	86	58	是	2	0	0	2	1
金山云	226	368	30	是	4	0	0	0	0
上海斐讯	227	33	70	是	0	1	0	0	0
中兴通讯	228	409	83	是	1	0	4	7	6
甘肃万维信息技术有限责任公司	245	8	14	是	9	0	0	2	0
北京万国长安科技有限公司	335	0	9	是	4	0	0	1	0
行业平均值	580	326	67		2.67	164.5	15.25	49.47	2

发生占比		37.14%	40%	70%	21.43%	8.6%	11.43%	21.43%	10%

我们从风险值风险等级、网络攻击、安全漏洞、隐私保护、恶意代码、僵尸网络、IP 黑名单、端口高危风险、SSL 高危风险等九个维度的网络风险数据对处于网络风险较高的七家取样企业做了分析，根据上表发现，2017 年年中至 2018 年 7 月底结束，北京光环新网科技股份有限公司面临的互联网风险最高；40%的云服务商出现安全漏洞；庞大的线上业务量使电商平台遭受 DDoS 攻击占比达到 37.14%；总体域名隐私泄漏高达 70%；恶意代码、僵尸网络、SSL 高危风险相对发生率较低；其中 21.43%的云服务商出现恶意代码，一旦企业发生恶意代码或僵尸网络事件，都可能导致业务中断事件；目前 11.43%的企业在 IP 地址被列入国际黑名单中，收录国际黑名单的安全设备将会阻断黑名单中 IP 地址的通讯，对线上业务的开展造成很大不良影响。

第4章 云服务商安全漏洞分析

4.1 云服务商最常见安全漏洞分析



4.2 安全漏洞详细统计和描述

漏洞详细信息如下：

安全漏洞 TOP10	数量	描述
OpenSSH 写入错误漏洞 CVE-2017-15906	371	在 7.6 之前的 OpenSSH 中的 sftp-server.c 中的 process_open 函数不能正确地阻止只读模式下的写入操作，这允许攻击者创建零长度文件。
OpenSSH 数据结构初始化漏洞 CVE-2014-1692	279	在 OpenSSH 到 6.4 的 schnorr.c 中的 hash_buffer 函数，当修改 Makefile.inc 以启用 J-PAKE 协议时，不会初始化某些数据结构，这可能允许远程攻击者导致拒绝服务（内存损坏），或者未指定的其他影响通过向量触发错误条件。
OpenSSH J-PAKE 授权问题漏洞 CVE-2010-4478	278	SSH 协议族可以用来进行远程控制， 或在计算机之间传送文件。与 OpenSSL 无关。
OpenSSH 敏感信息泄露漏洞 CVE-2016-0777	278	在 OpenSSH 5、x、6 x 和 7 .x 之前的客户机中 RAMEngYUn.Client 函数允许远程服务器通过请求传输整个缓冲区来从进程存储器中获取敏感信息，如通过读取私钥所示

OpenSSH 获取敏感信息漏洞 CVE-2012-0814	277	Auth-options.c 中的 auth-options.c 函数在 5.7 以前的 OpenSSH 中的 sshd 中提供了包含 authorized_keys 命令选项的调试消息，它允许远程认证用户通过阅读这些消息来获取潜在的敏感信息，如 Gitolite 所要求的共享用户帐户所示。注：这可以跨越特权边界，因为用户帐户可能故意没有 shell 或文件系统访问权限，因此可能没有受支持的方式来读取其主目录中的 authorized_keys 文件。
OpenSSH TCP 连接限时漏洞 CVE-2010-5107	277	OpenSSH 到 6.1 的默认配置强制建立 TCP 连接和完成登录之间的固定时间限制，这使得远程攻击者通过定期创建许多新的 TCP 连接更容易导致拒绝服务（连接时隙耗尽）。
OpenSSH 获取秘钥信息漏洞 CVE-2011-4327	277	ssh-keysign.c 在 ssh-keysign 中，在 5.8p2 之前的 OpenSSH 中，在某些平台上执行带有意外打开文件描述符的 ssh-rand-helper，允许本地用户通过 ptrace 系统调用获取敏感密钥信息。
OpenSSH 拒绝服务漏洞 CVE-2011-5000	277	当启用 gssapi-with-micon 认证时，OpenSSH 5.8 及更早版本中的 gss-serv.c 中的 ssh_gssapi_parse_ename 函数允许远程认证用户通过特定长度字段中的较大值导致拒绝服务（内存消耗）。 注意：此问题相关的情况可能有限。
sftp-glob.c/sftp.c 身份验证漏洞 CVE-2010-4755	277	在 FreeBSD 7.3 和 8.1，NetBSD 5.0.2，OpenBSD 4.7 和其他产品中使用的 sftp-glob.c 中的（1）remote_glob 函数和 OpenSSH 5.8 及更早版本中的 sftp.c 中的（2）process_put 函数允许远程身份验证的用户通过不匹配任何路径名的精心设计的 glob 表达式导致拒绝服务（CPU 和内存消耗），如 SSH_FXP_STAT 请求到 sftp 守护程序的 glob 表达式所示，这是与 CVE-2010-2632 不同的漏洞。
OpenSSH 拒绝服务漏洞 CVE-2016-10708	276	sshd 在 7.4 之前的 OpenSSH 中允许远程攻击者通过一个不按顺序的 NEWKEYS 消息导致拒绝服务（NULL 指针解引用和守护进程崩溃），正如 Honggfuzz 所示，与 kex.c 和 packet.c 相关。

4.3 SSL 高危风险

公司名称	SSL 高危
中兴通讯股份有限公司	6
北京光环新网科技股份有限公司	2
新网数码	2
万达信息股份有限公司	1
苏宁云商集团股份有限公司	1

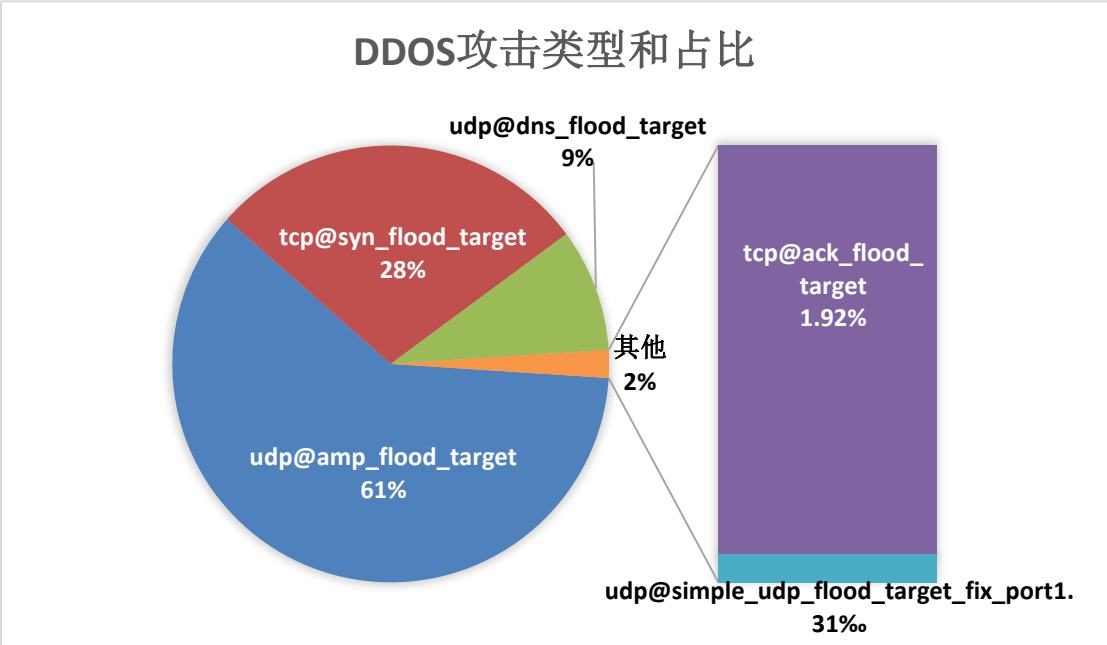
深圳前海小鸟云计算有限公司	1
海南易建科技股份有限公司	1

根据上表中数据，我们可以发现，中兴通讯股份有限公司的 SSL 高危漏洞数量最多，需加大管理力度和准备预防措施。在网络层针对数据应用的网络架构和系统入口进行安全防护，可采用的防护手段主要有防火墙和入侵检测。在适当的协议层进行访问规则和安全审查，将符合通过条件的报文从网络接口送出，对不符合的报文则予以阻断。企业可以通过以上对安全防护合理补充，帮助系统快速发现网络攻击的发生，扩展系统管理员的安全管理能力，提高信息安全基础结构的完整性。

一般数据加密使用的是 SSL（Secure Sockets Layer，安全套接层），通过加密实现数据集的节点和应用程序之间的数据保护。SSL 协议漏洞与 SSL 证书本身是无关的。SSL 证书用于激活服务器和客户端之间的 SSL 传输协议。现有的 SSL 协议已发展出 SSLv2、SSLv3、TLSv1、TLSv1.1 及 TLSv1.2 多个版本。其中 SSLv2 及 SSLv3 已被发现存在漏洞，推荐在服务器端配置关闭该协议，仅开启 TLSv1、TLSv1.1 及 TLSv1.2 即可避免受到漏洞影响。

第5章 网络攻击分析

5.1 云服务商 DDoS 攻击概况

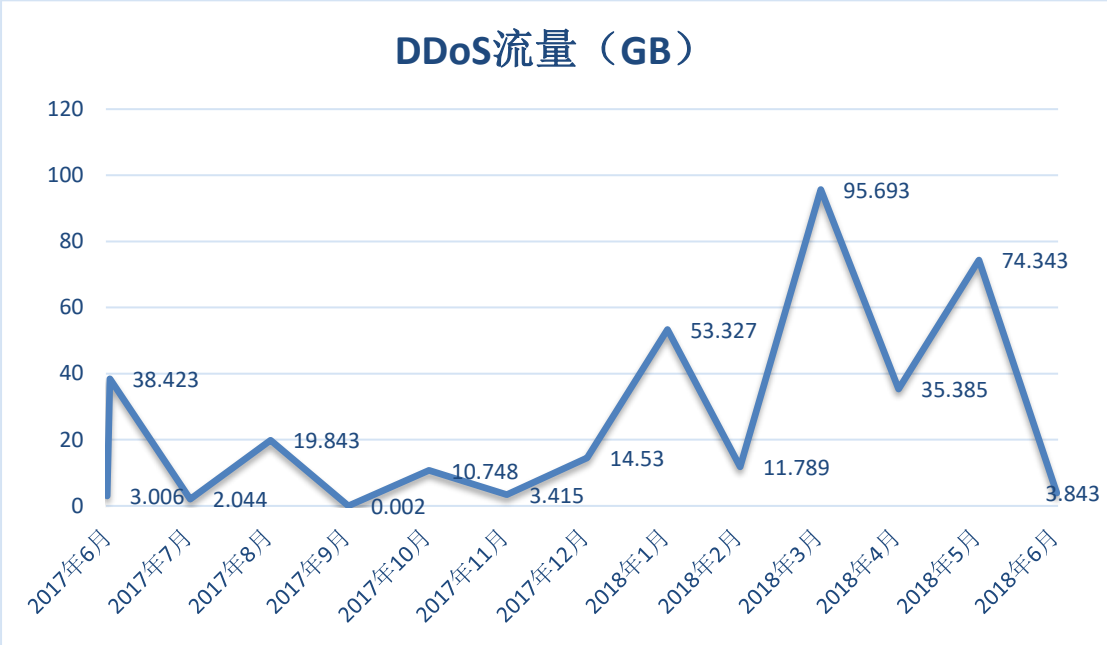


DDoS 攻击概况

DDoS 攻击类型	次数	占比
udp@amp_flood_target	**6893**	**60.5%**
tcp@syn_flood_target	3230	28.35%
udp@dns_flood_target	1037	9.1%
tcp@ack_flood_target	219	1.92%
udp@simple_udp_flood_target_fix_port	15	1.31‰

根据上表结果，云服务商一年内共遭受了 11394 次 DDoS 攻击。其中 TCP 半连接攻击占据网络攻击的主要部分，对于这种类型的 DDOS 攻击，可通过缩短 SYN 响应时间或设置 SYN Cookie 过滤 TCP 包等手段来实施。对于 UDP 放大攻击，可以通过限制 UDP 包大小，或建立 UDP 连接规则来达到过滤恶意 UDP 包，减少攻击发生的效果，具体可根据企业自身的详细情况选择合适的解决方案。

5.2 云服务商 DDoS 攻击流量年度统计情况



2017 年 6 月至 2018 年 7 月截止，安全值统计了 70 家提供云服务的公司，根据表中数据绘制上图。从图中可以得出，分别在 2017 年 7 月、2017 年 9 月、2018 年 2 月、2018 年 4 月、2018 年 6 月发生了 5 次攻击流量的爆发，其中 2018 年 4 月 DDoS 攻击流量达到 95.693G 的峰值。根据近半年攻击流量，各企业需加强网络信息安全的意识，不可有丝毫的懈怠。

5.3 高危端口风险

开发人员和管理员应使用最佳工具保护设备及服务安全，拒绝使用非加密协议。使用 HTTPS 和 FTPS 可以最大限度减少潜在入侵者的攻击面，同时保护敏感数据的传输安全。此外，除了使用诸如 SSH 这类加密协议，还应在易遭受攻击的设备前配置防火墙，同时设置为仅通过 VPN 访问。若无法做以上部署，应设置强密码进行保护，切勿使用默认凭证。

完善数据存储管理制度。建立、健全账号口令管理、补丁管理、安全配置管理、防病毒管理等安全管理制度，定期进行安全检查和风险评估，对发现的安全漏洞、高危端口及时进行处理。信息使用设置可信域和非可信域，实施不同的安全策略，实现分层分级的安全防护。建立终端接入的审批流程，部署终端接入管理系统，确保安全维护人员的所有操作可审计、可追溯。

第6章 其他网络风险分析

6.1 HTTPS 证书过期

公司名称	云产品名称	HTTPS 证书过期
京东	京东	46
阿里云计算有限公司	阿里云	5
新网数码	新网云	4
北京光环新网科技股份有限公司	光环新网	4
苏宁云商集团股份有限公司	苏宁云	3
中兴通讯股份有限公司	中兴云	3
曙光信息产业股份有限公司	曙光云	3
深圳前海小鸟云计算有限公司	小鸟云	2
杭州质云科技有限公司	质云	1
北京易捷思达科技发展有限公司	EasyStack	1
甘肃万维信息技术有限责任公司	甘肃万维	1
北京万国长安科技有限公司	万国数据	1
北京金山云网络技术有限公司	金山云	1
深圳市证通电子股份有限公司	证通云	1
中国联通	沃云	1

HTTPS 实际就是在 TCP 层与 HTTP 层之间加入了 SSL/TLS 来为上层的安全保驾护航，主要用到对称加密、非对称加密、证书，等技术进行客户端与服务器的数据加密传输，最终达到保证整个系统的安全性。

网站的运行方式可以建立在 HTTPS 协议之上，以避免非加密数据在网络传输过程中所导致的被恶意截取、篡改、重定向等网络安全问题。云服务商需及时查询关注自身 HTTPS 是否过期，以更好的保证数据的完整性，确保数据在传输过程中不被改变，防止数据在中途被窃取。

第7章 附录

企业名单（按安全值升序排序）

编号	云平台名称	企业名称
1	光环新网	北京光环新网科技股份有限公司
2	新网	新网数码
3	京东	京东
4	阿里云	阿里云计算有限公司
5	苏宁云	苏宁云商集团股份有限公司
6	金山云	北京金山云网络技术有限公司
7	斐讯云	上海斐讯
8	中兴云	中兴通讯股份有限公司
9	甘肃万维	甘肃万维信息技术有限责任公司
10	万国数据	北京万国长安科技有限公司
11	网易云	杭州质云科技有限公司
12	证通云	深圳市证通电子股份有限公司
13	UCloud	上海优刻得信息科技有限公司
14	天翼云	中国电信
15	万达信息	万达信息股份有限公司
16	中企通信	中企通信
17	青云	北京优帆科技有限公司
18	太极云	太极计算机股份有限公司
19	小鸟云	深圳前海小鸟云计算有限公司
20	华为云	华为
21	云端网络	云端网络
22	EasyStack	北京易捷思达科技发展有限公司
23	睿江云	广东睿江云计算股份有限公司
24	鹏博士	鹏博士
25	网宿云	网宿科技
26	宝德云	宝德云
27	SpeedyCloud	北京迅达云成科技有限公司
28	汇智云	汇智软件
29	沃云	中国联通
30	海南易建	海南易建科技股份有限公司
31	大唐网络	大唐网络
32	宝信软件	宝信软件
33	首信	首都信息发展股份有限公司
34	有孚网络	有孚网络
35	森华易腾	森华易腾
36	曙光云	曙光信息产业股份有限公司

37	中联润通	中联润通
38	亿林网络	亿林网络
39	云科数据	内蒙古云科数据服务有限公司
40	海云捷迅	北京海云捷迅科技有限公司
41	360 云	360
42	北京供销大数据	北京供销科技有限公司
43	立思辰银山	立思辰银山
44	临沂拓普	临沂拓普
45	国裕数据	国裕数据
46	国云科技	国云科技
47	兴业数金	兴业数金
48	华云数据	华云数据
49	神州数码云	神州数码云
50	上海科技网络	上海科技网络
51	蓝汛云	蓝汛
52	国研网络	国研网络
53	腾讯云	腾讯
54	美团云	美团
55	移动云	中国移动
56	首信科技	北京首都在线科技股份有限公司
57	浪潮云	浪潮
58	上海宽惠	上海宽惠
59	中金数据	中金数据
60	山东众志	山东众志
61	未来国际	未来国际
62	快云	快云
63	百度云	百度
64	世纪互联	世纪互联
65	国富瑞	国富瑞
66	阅联	阅联
67	犀思云	犀思云
68	联想云	联想
69	互联港湾	互联港湾
70	达闼科技	达闼科技