《阿里云安全报告》中文版开启全文下载，详解2018上半年网络安全态势

阿里云安全技术 / 2018-10-29 13:47:00 / 浏览数 2853 安全技术 技术讨论 顶(0) 踩(0)

近日，由阿里云安全创新实验室推出的《2018上半年阿里云安全报告》中文版开启全文下载。

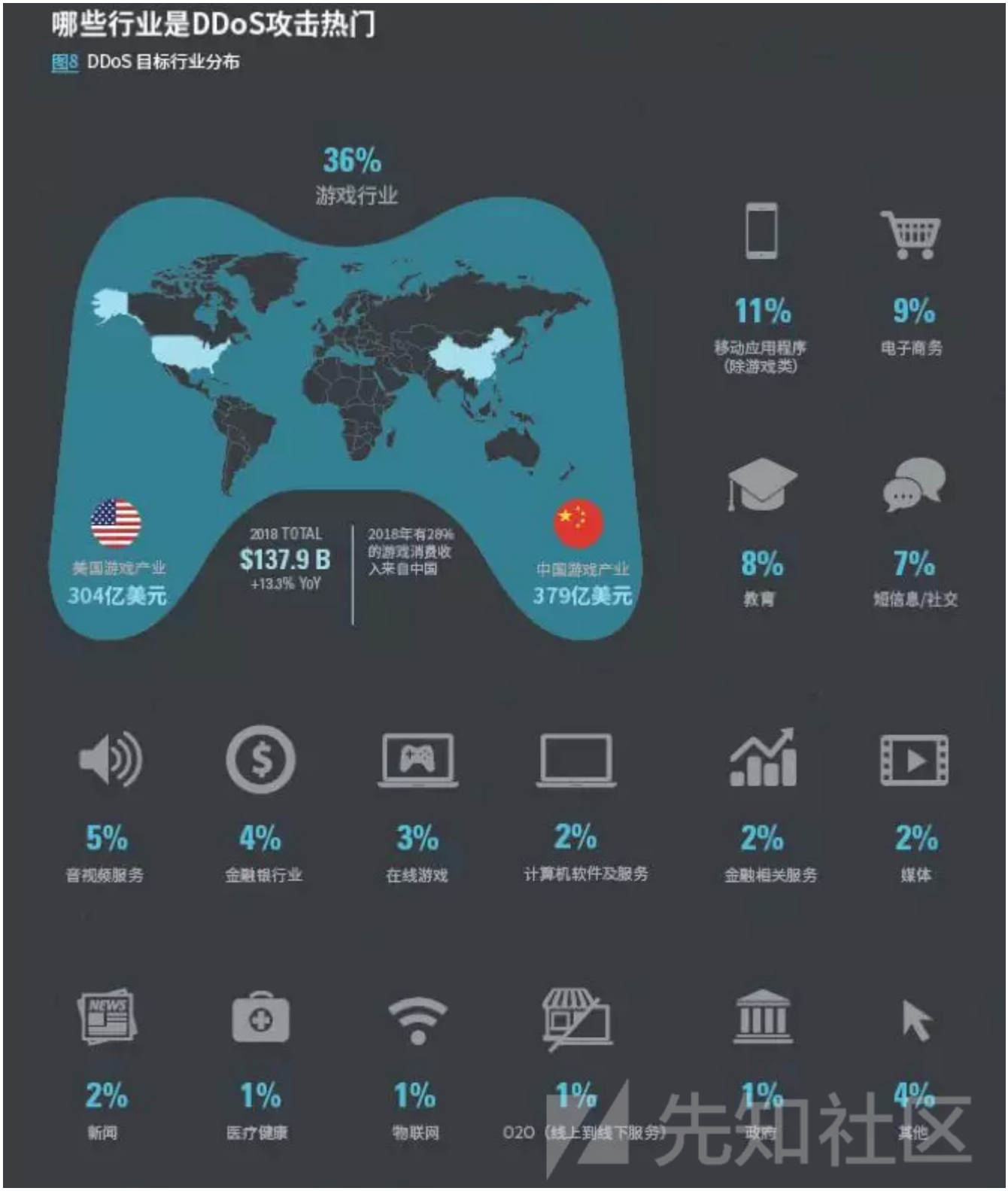
报告指出，今天的网络安全风险比以往任何时候都大，无论企业的服务和数据部署本地还是云上，只要有价值的数据，就会成为攻击目标。在云上，企业可以借助云服务商
报告部分亮点观点

过去十年，绝大多数入侵行为背后的主要原因有三类：人为失误、暴露在互联网上的漏洞、公司网络或终端节点的安全方案无法及时识别恶意软件。网络入侵的主要原因并不
云部署改变了一切，但攻防之战仍和以前一样：双方之间的安全工具之战在无限升级。
利用可自适应的机器学习驱动的安全与少量人工参与相结合是未来的发展方向。

报告部分亮点数据

01.DDoS攻击

阿里云在 2018 年看到的 DDoS
攻击强度和复杂度均打破了历史记录，仅在2月份就抵御了数次Memcached攻击，峰值超过800Gbps，每秒TB级别的攻击时代已经到来。游戏、移动应用、电子商务等竞争



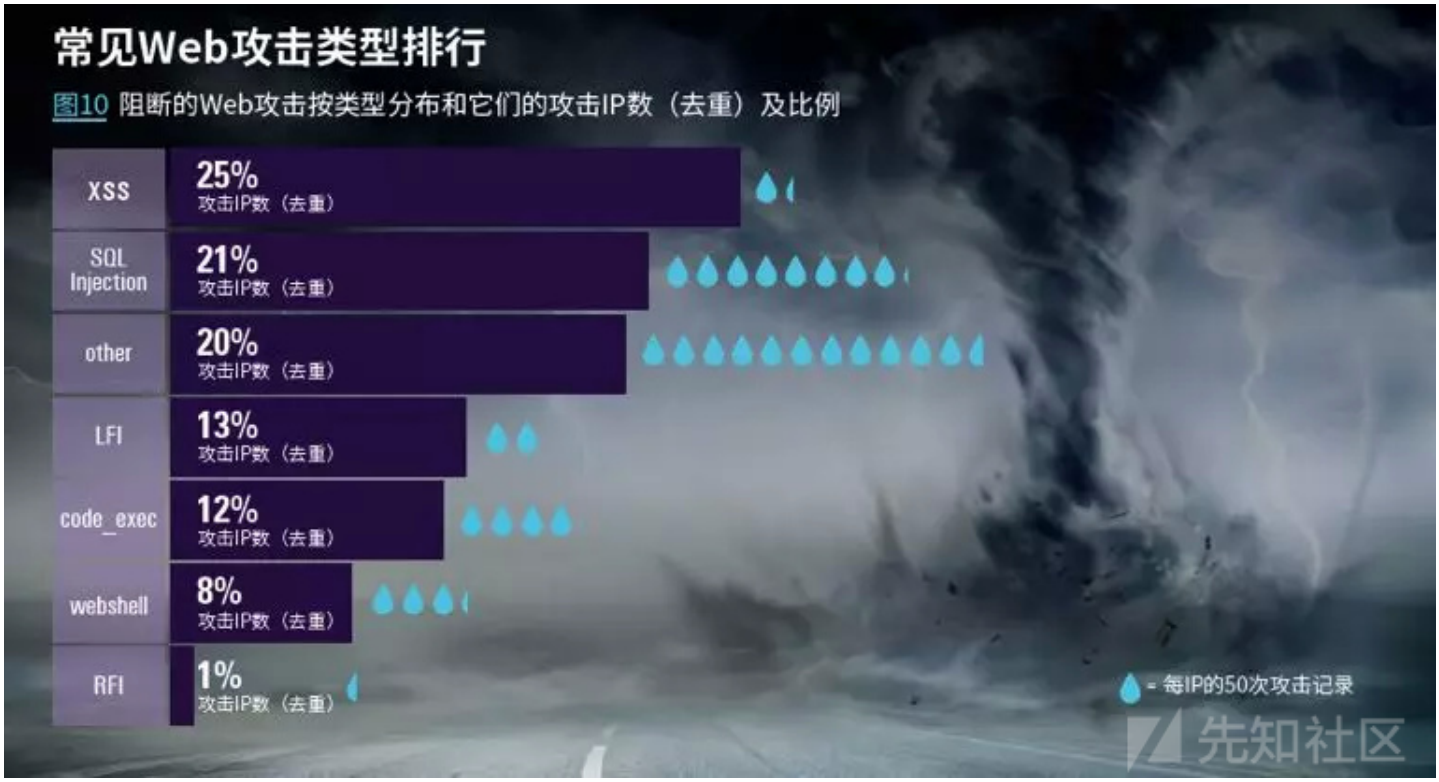
当DDoS攻击变得越来越猛烈的时候，攻击防护设施很快达到其容量极限，而云防护能力的高扩展性则不存在这个问题。

阿里云通过自主开发的DDoS防护服务可以保障阿里云所有数据中心的安全，通过自动检测并将DDoS攻击牵引到远离用户网络基础设施的地方。从攻击发现、流量路由到流

在《DDoS攻防：一场古老战争的"新发展"》一文中，我们对DDoS攻防的新趋势及云上DDoS最佳实践做了详细解读。

02.基于Web的攻击

2018 上半年，阿里云检测并阻止了五千亿次以上的 Web 攻击。平均每天有 30 亿次攻击，这些攻击来自 200 万个以上的唯一 IP 地址。阿里云 WAF 阻止的两个最流行的攻击是 XSS 和 SQL 注入。

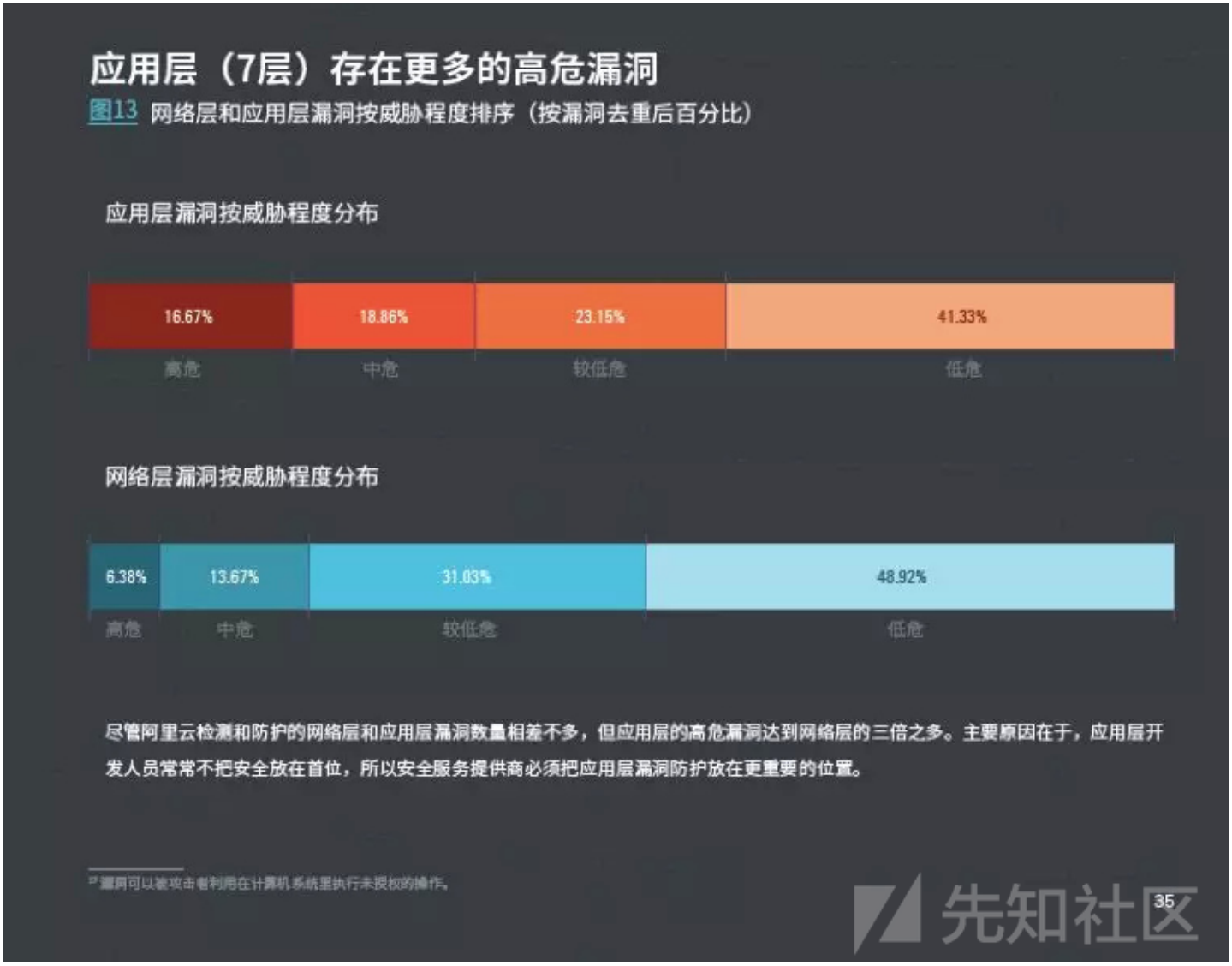


云端WAF（而非本地WAF）可以提供针对性更强更有效的解决方案，因为云端WAF具有更好的扩展性、更经济高效并且更易于实施。

报告数据显示，基于深度学习的WAF不仅节约了人工成本，而且使用正则加深度学习双引擎的WAF的准确率提升到99.999%，这相对于仅使用正则的WAF99.99%的准确率

03.漏洞检测

报告显示，在过去十年中，许多最重大的数据泄露都始于安全漏洞，与本地部署相比，云部署的关键安全优势之一在于云提供商使用中央管理来确保安全系统始终保持最新，



以著名的比特币勒索事件为例，阿里云安全团队在“Eternal Blue”漏洞公布的第一时间就完成了对受影响用户的预警并提供了修复方案，通过全球访问策略控制，确保所有用户避免受到漏洞攻击。一个月后，Wannacry勒索事件爆发

下载报告全文了解更多精彩内容，报告获取方式：

1. 打开阿里云官网，点击底部的信任中心即可看到报告下载链接
2. 直接复制链接到浏览器：https://security.aliyun.com/trust?spm=5176.8142029.631162.38.e9396d3e5qG0zj

上一篇：使用COM将代码注入到受Windo... 下一篇：Windows通知功能(WNF)妙用

1. 0 条回复
   - 动动手指，沙发就是你的了！