

2015年度 云盾态势感知报告

YunDun 2015 Annual Report for Security Situation Awareness





目 录

1	执行摘要.....	5
2	核心发现.....	8
3	高级威胁	12
3.1	Web 定向攻击	12
3.2	撞库攻击.....	13
3.3	IP 信誉库.....	15
3.4	新型威胁预测.....	18
4	Web 应用攻击.....	20
5	暴力破解攻击	25
6	恶意文件	29
7	案例	33
7.1	解密 BBOSS 组织大规模挂马事件.....	33
7.2	PostgreSQL 弱口令致使数千台服务器沦陷.....	35
7.3	黄赌毒挂马事件	37
8	总结	40
	附录：2015 年全球十大网络安全事件.....	42

PART
ONE

执行摘要

DT 时代，信息安全问题的解决已经慢慢演化成对安全大数据分析能力的挑战，大规模的安全数据需要进行有效的关联、分析和挖掘才能产生最终价值。基于此，阿里云于 2015 年 7 月发布了云盾安全态势感知服务。态势感知让攻击受害者第一次具备了反击能力，以及对于全局威胁的可见性和集中管控能力。

作为一个集合了大数据和安全的跨界产品，云盾态势感知系统不仅拥有 PB 级别的大数据分析和计算能力，而且通过机器学习，汇集全网安全数据以及威胁情报，建立了完整和智能安全威胁模型，作用到百万客户的实际业务场景中。通过对海量数据的收集、分析与展现，帮助客户获得更好的全局可见性和安全智能，从而抵御来自各个维度和领域的新型安全威胁。

2015 年度云盾态势感知报告聚焦在数据中心云计算用户面临的高级持续威胁、定向 Web 应用攻击、面向系统的暴力破解以及主机恶意文件四个方面的新威胁和安全趋势。

阿里云是国内最大的公共云计算服务提供商。保护了中国 30% 的网站。作为一个集合了大数据和安全的跨界团队，云盾不再用传统的方法去解决

信息安全问题，而是通过海量数据的收集、分析与展现，帮助企业获得更好的全局可见性和威胁发现能力，按攻击者的视角来建立安全防御体系，来抵御来自四面八方的新型安全威胁和内部人员的监守自盗。

态势感知团队通过对网络攻击持续的分析与研究，发布云盾态势感知2015 年度报告。

PART
TWO

核 心 发 现

发现 1：账号和密码隐私泄露形势更加严峻，金融类网站成为重灾区。

从云平台每天遭受数千起撞库攻击可以看出，大量的用户私密数据已被黑客窃取并用于攻击更多的网站。随着互联网金融的蓬勃发展，金融类网站已然成为首要攻击目标。

发现 2：黑色产业链愈发猖獗，破坏行为多样化。

为获得更多的利益，黑客入侵后除了“拖库”和植入后门外，新型的破坏行为层出不穷，更加多样化。如，在阿里云安全团队的监控中，入侵服务器后在篡改页面插入各种赌博色情广告的案例同比上升 50%，也监控到在被入侵的网页中插入恶意的 Javascript 用于发起 CC 攻击的案例。

发现 3：自动化 Webshell 黑客工具提升入侵效率，入侵成功仅需 1 小时。

自动化批量扫描 Webshell，这种低成本高收益的攻击方式在 2015 年迅猛增长，相比 2014 年翻了 10 倍。自动化扫描工具也越来越丰富，一句话木马的检测和绕过对抗进一步升级。

发现 4：数据库应用被利用的事件数量增多，将成为下一个黑客入侵的突破点。

MySQL 弱口令 UDF 提权已经被广泛用于抓“鸡”，黑客又将目标瞄准了其他的数据库服务，PostgreSQL 弱口令漏洞和年底爆发的 Redis 未授权漏洞给互联网带来了一场血雨腥风。

发现 5：弱密码导致主机被入侵案例数量最多，用户在整体安全意识上较去年没有明显的改进。

黑客入侵成功的案件中，由弱密码导致的最多，暴力破解攻击成为黑客最喜欢使用的攻击手法，互联网发展到今天依然没有很好地解决身份安全认证的问题。

发现 6：漏洞扫描演变为分布式集群化，不少开放式毫无限制的漏洞扫描引擎沦为黑客工具。

代理扫描已从单机模式发展成为集群模式，高效的扫描方式为 CC、撞库等攻击提供源源不断的“子弹”。黑客也不再是孤军奋战，“买家”、“卖家”和“中间人”等角色各司其职，一条成熟的地下产业链已经形成。

PART
THREE

高级威胁

3 高级威胁

态势感知是云盾的“眼睛”，它用大数据分析来颠覆传统单一的入侵和漏洞检测。在 2015 年中，阿里云安全专家根据现有网络攻击形势评估，按攻击者的视角来建立安全防御体系，从纷杂的访问数据中，抽丝剥茧地分析出黑客的独特行为，帮助客户感知到当前遇到的安全威胁，用大数据分析挑战传统安全亟待解决的困扰。

3.1 Web 定向攻击

为了解决“告警无数然并卵”的困扰，阿里云安全团队研发了 Web 定向攻击模型，用于识别对客户真正产生威胁的攻击。针对每小时数十亿流量进行分析，第一时间向用户推送告警信息。上线以来共捕获累计超过 8 万个定向攻击者，其中入侵成功率为 12.19%。

我们做了一个有趣的统计，对黑客入侵一个网站所花费的时间进行分析，发现半数黑客只用了不到一个小时就完成了整个入侵过程。从下图可见，半数黑客从开始攻击到攻破系统仅需 1 小时。

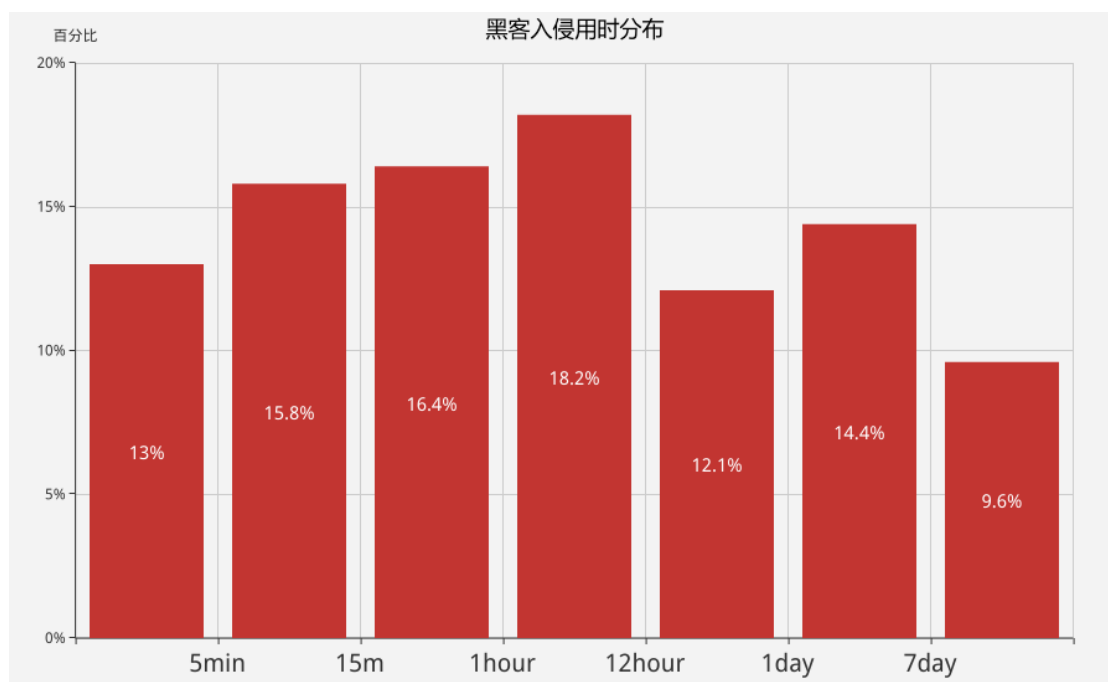


图 3-1 黑客入侵用时分布

3.2 撞库攻击

在某邮箱数据库泄露事件之后，撞库这种攻击方式逐渐得到了攻击者的青睐。从撞库检测模型上线之日起，日均检测攻击事件数千起，每起攻击事件平均包括数千次撞库登录请求。进一步统计，每天发起的攻击事件里，账号密码组合去重后仍有几十万对。更严重的是，这些账号密码组合就像黑客的弹药库一样，随着更多的企业被拖库而不断的更新迭代。无数用户的个人账号被黑客通过“撞库”偷窃，用于发站内广告和黄色信息，企业的正常业务受到严重影响。

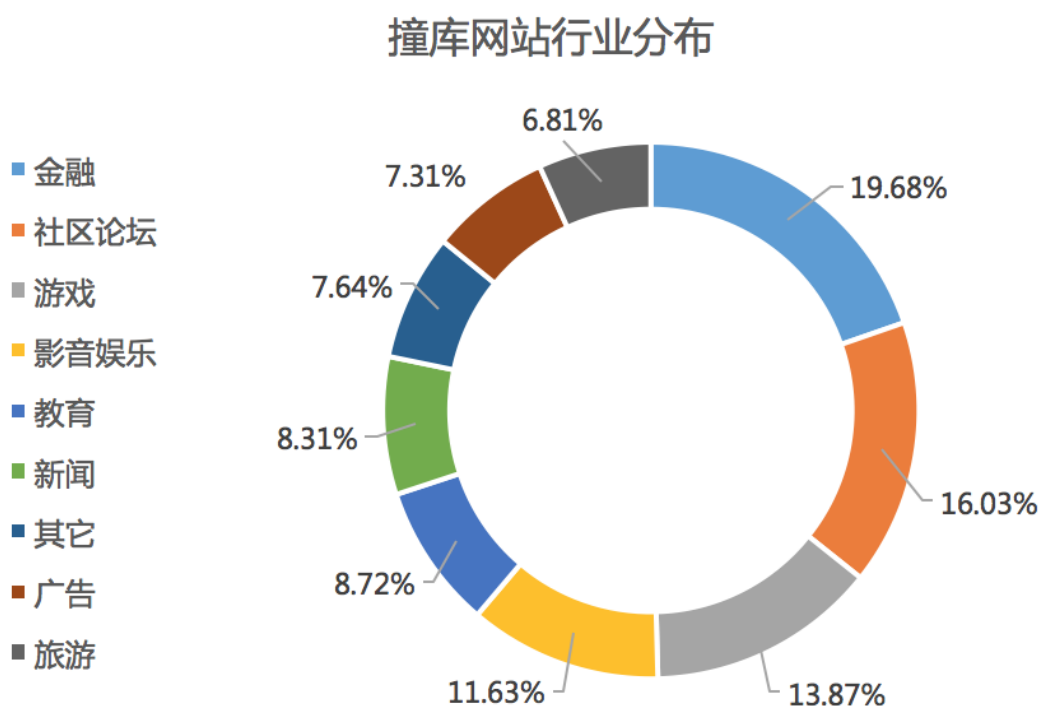


图 3-2 撞库网站行业分布

上图是阿里云安全团队对开通了态势感知的受害网站进行的统计，可以看见经常遭遇撞库攻击的网站里，排名前三的行业分别为金融(19.68%)、社区论坛(16.03%)、游戏(13.87%)，几乎占据了全部攻击的一半，接着为影音娱乐、教育、新闻、广告、旅游等行业。

数周前，阿里云安全团队帮助一个云上客户应急响应，查明客户遭受了撞库攻击，网站用户的代金券被攻击者一洗而空。经过进一步的调查，发起攻击的 IP 有数百个之多，且证据都指向了一个在互联网上经常遭到投诉，

从 2014 年开始扫描代理的服务器。经过取证和分析，发现服务器上存储了近 300GB 的各类数据，仅仅代理服务器的数据就有 90 多 GB，除了扫描到的代理服务器，还有各类弱口令肉鸡数据。回顾整个黑产业链路，扫描代理，出售代理，收集社工库到最终发起撞库攻击，不同的环节由不同的角色来完成，说明撞库攻击早已不是一两个黑客兴起玩玩的把戏，已经成为了一项发达而成熟的黑色业务。

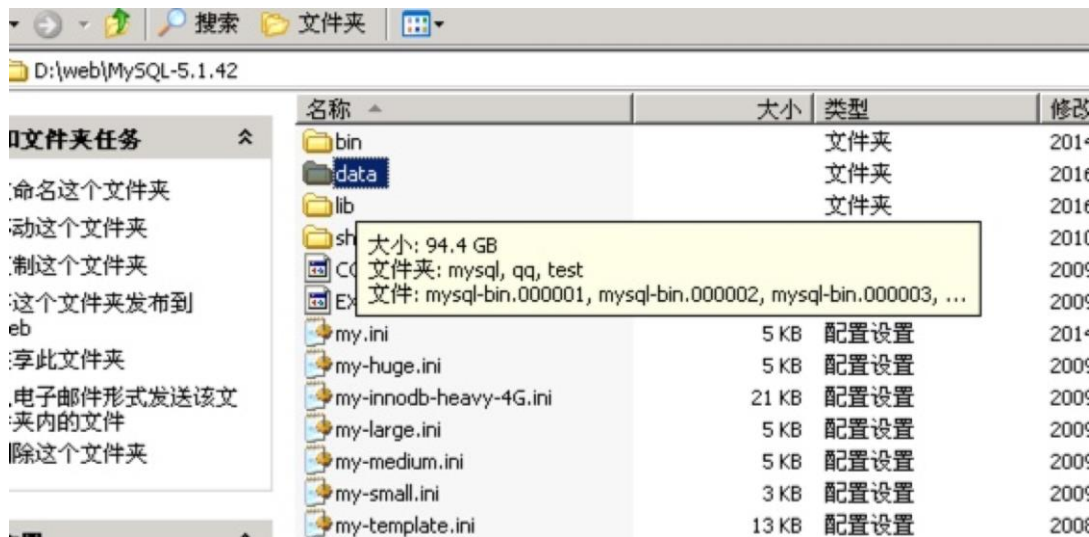


图 3-3 黑客非法所得截图

3.3 IP 信誉库

在数据积累方面，阿里云安全团队将所有历史攻击数据进行聚合和建档，沉淀为 IP 信誉库。当一个 IP 的信誉较差时，即使只是访问了一下网站后

台，我们都会对其行为进行分析，及时进行风险评估并且将结果提供给用户。

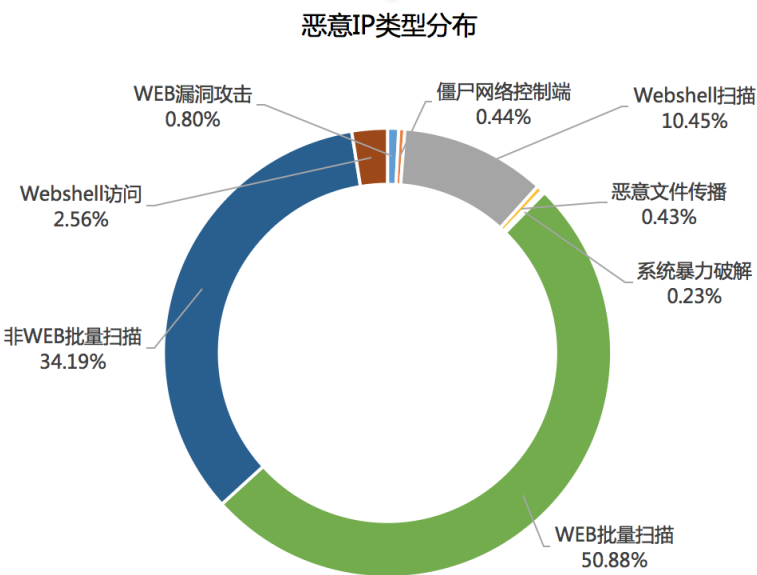


图 3-4 恶意 IP 类型分布

截至目前，阿里云安全团队已经收集了超过 50 万个恶意 IP。其中半数 IP 都经常性进行 Web 批量扫描。

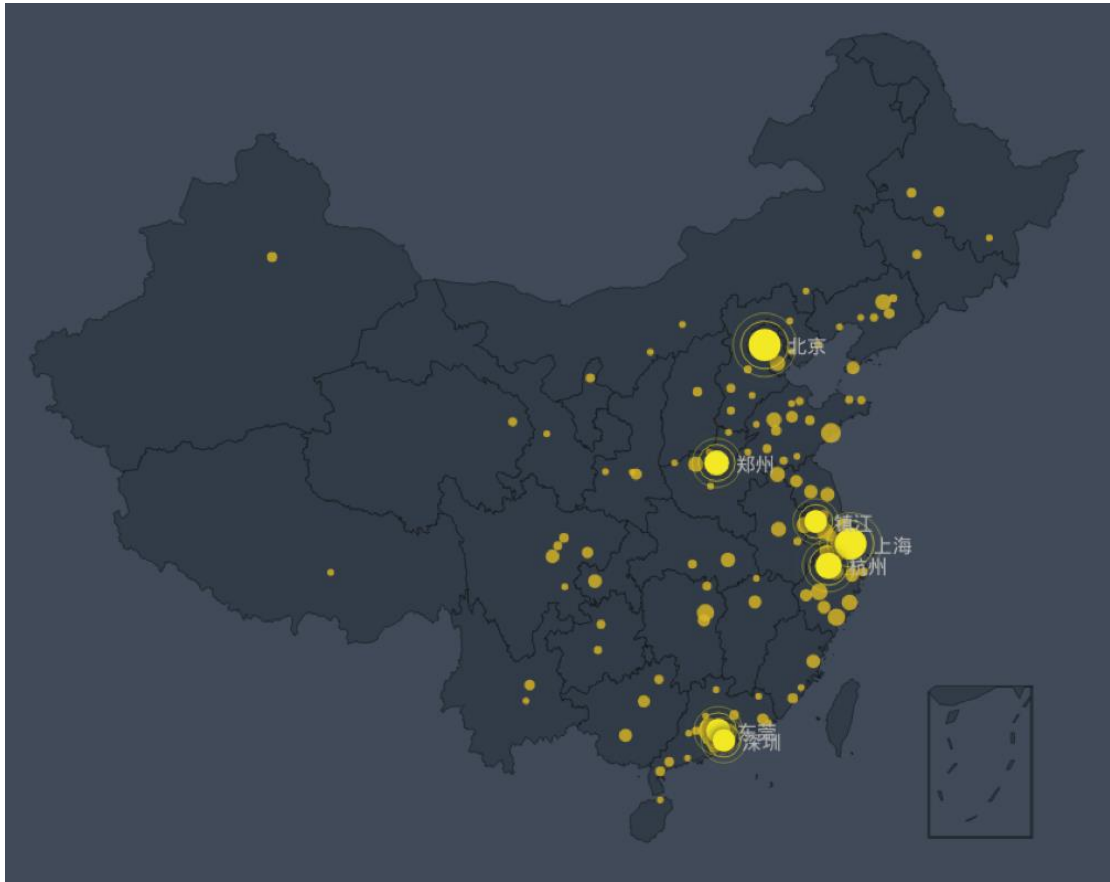


图 3-5 恶意 IP 地理位置分布（国内）

从全球角度去看，恶意 IP 数量排名前三的国家是中国、美国和俄罗斯。抽取国内的恶意 IP 进行分析，它们主要分布在沿海的发达地区，在黑客圈内十分有名的“镇江”机房赫然上榜。

3.4 新型威胁预测

可以预见的是，在 2016 年，随着传统攻击防御手段的丰富和广泛采用，使得攻击者收益下降，导致越来越多诸如“撞库攻击”，“鱼叉攻击”，“水坑攻击”等新型威胁；另外，随着账号密码安全越来越严峻，网络盗号，社工攻击也会越来越频繁。对于此类威胁，除了第一时间识别黑客的“撞库攻击”行为，阿里云安全专家也会及时推出更具针对性的安全解决方案。

PART
FOUR

WEB应用
攻击

4 Web 应用攻击

2015 年度 Web 应用攻击总体呈现上升趋势，全年攻击次数超过 80 亿次。按季度进行统计，从第一季度不到 6 亿次/月上升到第四季度高于 8 亿次/月。在双十一当天，Web 应用攻击达到了全年的峰值 8000 万次/天。

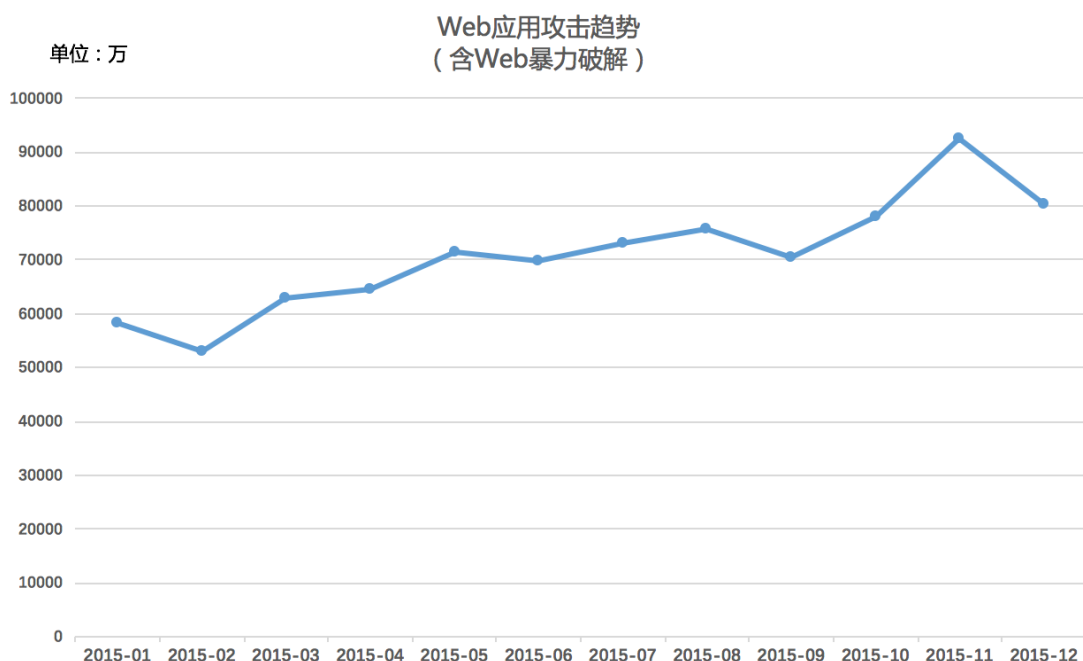


图 4-1 Web 应用攻击趋势

从攻击类型上看，“命令执行”类型的 Web 攻击占到总数的 31%，超过“SQL 注入”攻击这一最古老的攻击方式，上位成为最受黑客喜爱的攻击方式。“命令执行”攻击被黑客所热衷，是由于这是一种杀伤力极强的攻击行为，

攻击一旦得手，即意味着黑客可以控制目标服务器，相对于其他攻击类型来说，它是获取服务器系统权限最便捷的途径。

值得一提的是，云盾监控表明，96.25%的 web 攻击均由漏洞扫描器发起，有大范围和批量性的特征，但其攻击力度很低，能够被大多数 WAF 应用防火墙所拦截。对于剩下的 3.75%的攻击行为，则是由黑客手动发起的攻击，这种类型攻击，更具有破坏性和针对性，经常带有 0day 漏洞的攻击特征，通用配置下的 WAF 设备无法拦截，需要企业引起重视。

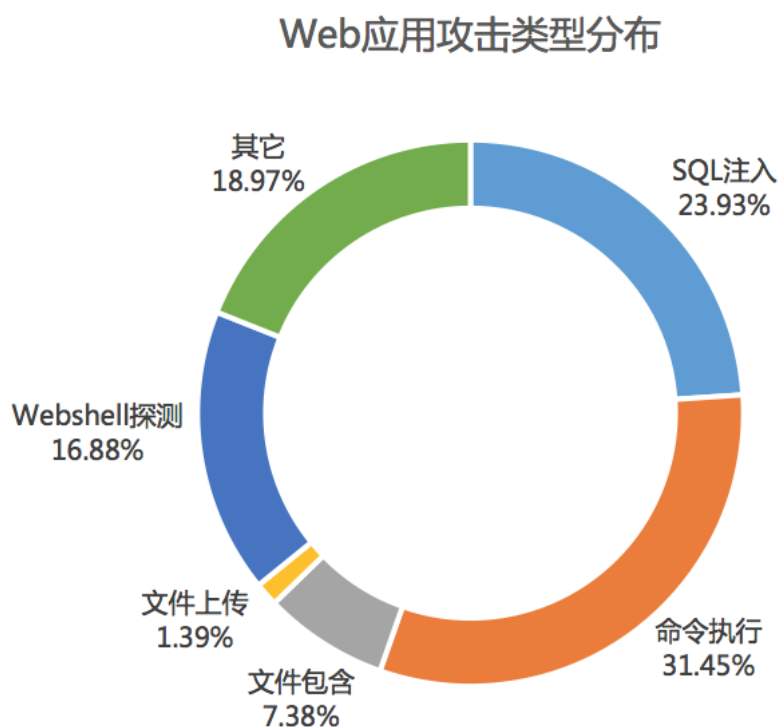


图 4-2 Web 应用攻击类型

另外，“Webshell 探测”的攻击类型引起了阿里云安全团队的关注。从监控数据上看出，“Webshell 探测”攻击增长迅猛，7 月的时候只有 2000 万次，到了年底已经突破 8000 万次/月，增长率高达 400%。造成攻击趋

势增加的原因，一方面得益于黑客的扫描工具传播越来越广泛；另一方面则由于高危漏洞频发，出现了多种新型的自动化入侵工具，黑客使用的 Webshell 都是固定的。我们预测，在 2016 年，互联网范围内黑客 Webshell 扫描的成功率会得到大幅提升。

决定黑客 Webshell 扫描的成功率很大一部分就是由他所用的密码字典决定的，阿里云安全团队将 2015 年的 Webshell 连接密码数据做了个统计，从中可以看出黑客最常用的密码是什么：

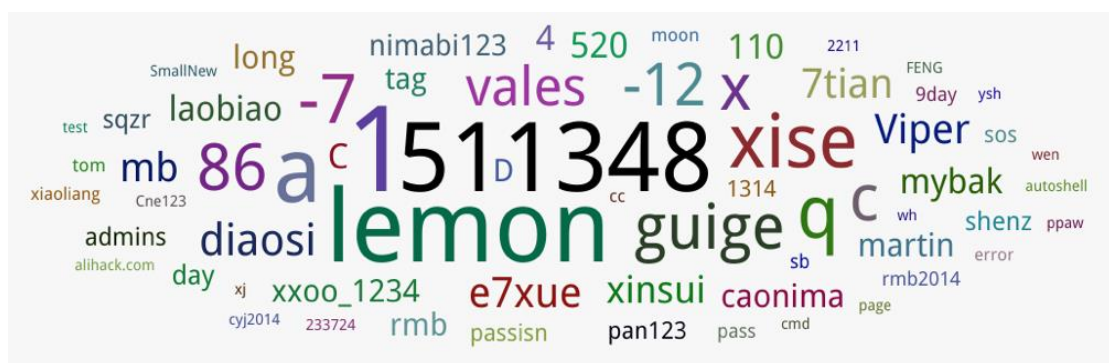


图 4-3 一句话 Webshell 密码使用占比

一直以来，大多数 WAF 都支持拦截常见的 Webshell 扫描请求，大大降低了该行为的成功率。但部分黑客已有新的对策，转变扫描策略，发送无害的请求（如 echo 一段简单字符串）进行扫描，从而绕过 WAF。当前一款新型 Webshell 管理工具，拥有丰富的自定义功能，可以对攻击代码进行任意的加密和混淆，也是一种绕过常规 WAF 的有效途径。

由此，阿里云安全团队预测 2016 年 Webshell 扫描将会持续增多，而常规 WAF 在 Webshell 连接请求方面的拦截成功率或识别率将受到极大挑战。

PART
FIVE

暴力破攻
解击

5 暴力破解攻击

暴力破解攻击成本极低，但成功率比 Web 攻击高出很多，一直以来都是黑客普遍采用的针对云服务器的攻击手法。

2015 全年云盾共拦截了 280 亿次暴力破解攻击，12 月的总攻击次数逼近 30 亿次。阿里云安全团队预测，2016 年暴力破解次数的峰值将突破 3 亿次/天，安全形势将更为严峻。

云服务器普遍默认安装 FTP 服务，且 FTP 暴力破解效率高，因此大部分黑客都将目标指向了 FTP 服务。全年 FTP 暴力破解攻击占比为 37.62%，超过远程登录服务（SSH、RDP）暴力破解次数的总和。

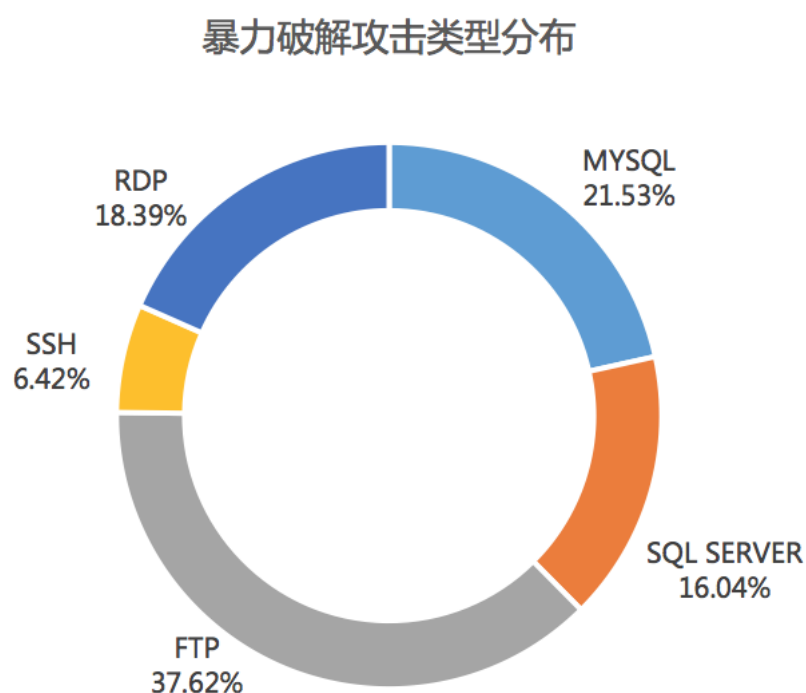


图 5-1 暴力破解攻击分布

除了 FTP 服务外，数据库的暴力破解攻击也是黑客最常用的攻击手法之一。过去一年内，以 MySQL、SQL Server 为主要目标的数据库爆破攻击次数也占到了总数的三分之一。

值得一提的是，一些用户量不及 MySQL 但应用也相当广泛的数据库应用，也开始成为黑客的攻击目标。11 月上旬，著名的非关系型数据库 Redis 被指可用于直接获取系统权限。在接下来的两天内，云盾态势感知检测到 Redis 非法连接数上涨了 200%，发起异常请求的源 IP 数也增加了一倍。这些 IP 先是批量扫描 Redis 数据库的默认端口，然后向服务器写入 SSH 公钥，最后通过 SSH 登录服务器，执行下载木马等恶意行为。虽然一周后 Redis 攻击趋势有所回落且趋于平缓，但从 12 月以来攻击次数一直稳步上升。

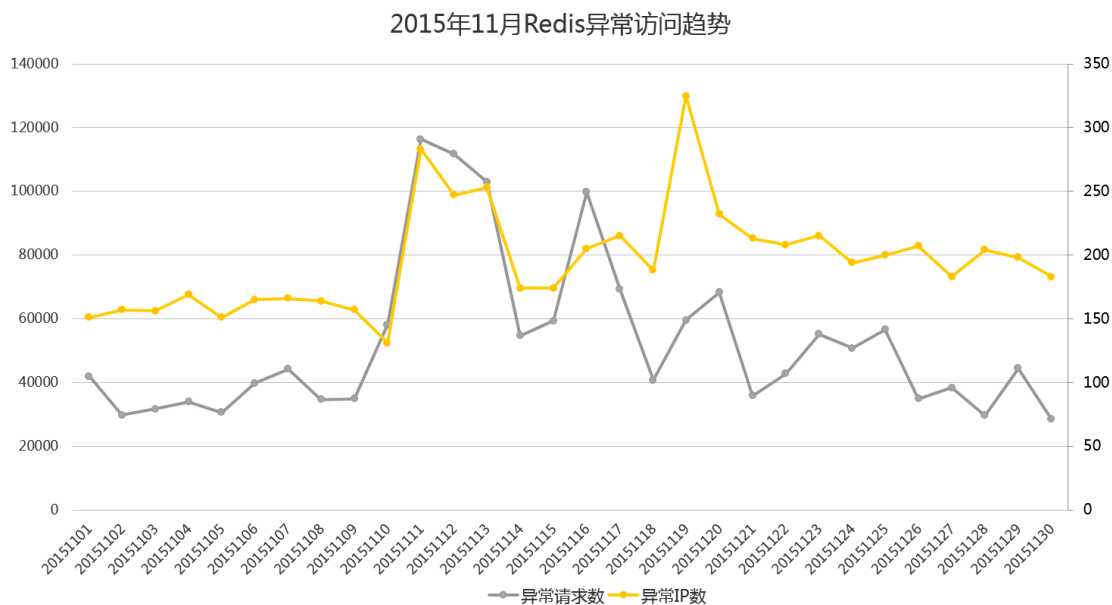


图 5-2 11 月 Redis 异常访问趋势

由此，阿里云安全团队预测，为了绕过防护软件的拦截措施，可获权限很高的应用，如 MySQL，Redis 等，将会成为黑客暴力破解攻击的新目标。

PART
SIX

恶意文件

6 恶意文件

云平台上每天都会发现大量的网页木马（Webshell），平均每天查杀的网页木马数以百计。黑客以 Webshell 作为跳板，进一步入侵和获取主机上的敏感信息，或安装恶意软件对其他用户发起网络攻击。

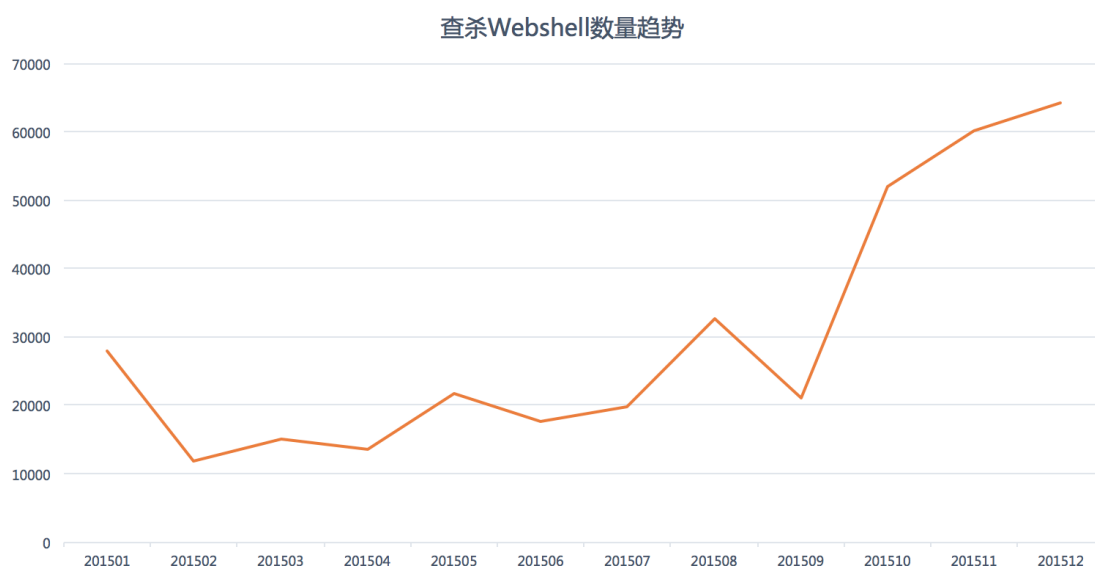


图 6-1 查杀 Webshell 数量趋势

从网页木马的文件类型上看，PHP 木马占总量的 48%，其次是 ASP。我们推断，云平台上 PHP 类型的网站较多，网站防护功能较弱，更容易被黑客入侵。

基于阿里云安全团队长期积累的攻击识别模型，云盾态势感知的自动化入侵回溯能够还原出大部分入侵事件的攻击路径。结果显示因弱口令原因而被植入网页木马的主机数量占到了绝大多数，从侧面反映了网站和服务

器管理人员仍需要继续增强密码意识。

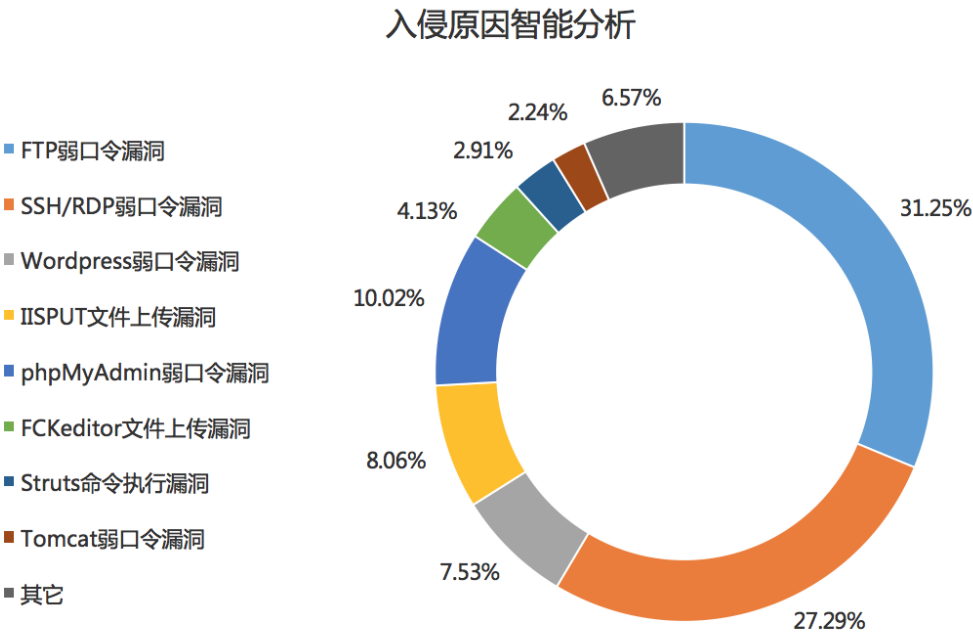


图 6-2 入侵原因智能分析结果

除了网页木马，恶意软件也是云服务器的一大安全威胁。攻击者通过多种攻击手段在服务器中植入恶意软件，组建僵尸网络并发起 DDoS、CC 攻击等恶意行为。2015 年云盾共发现数千个僵尸网络控制端，阻断了它们与“肉鸡”的通信，保障了阿里云服务器不被用于发起恶意攻击。

很少攻击途径可以让黑客直接向服务器上传恶意软件，因此大部分的恶意软件都是其它服务器上获取。借助大数据的分析能力，2015 年云盾态势

感知系统共发现恶意文件传播源 3015 个，对它们进行了长期的监控。其中 70%以上的传播源使用了 HFS (HttpFileServer) Web 程序。HFS 程序体积小，使用方便，深受国内黑客喜欢。

在被传播的文件中，木马程序的数量仍占到绝大多数，可见对服务器进行长期控制仍然是黑客的首要目的。不过，有一部分 HFS 上面部署了与“挖矿”、“流量挂机”相关的工具。相对于控制机器，使用“肉鸡”运行“挖矿”、“挂机”等工具可以给黑客带来直接的经济利益，风险也相对较低。

PART SEVEN

案例

7 案例

7.1 解密 BBOSS 组织大规模挂马事件

2015 年末，阿里安全威胁情报中心监控到一起大面积网站挂马事件并给其取名为 BBOSS，受感染的网站数量全球范围内超过 12 万个，其中约 78% 都使用了开源 CMS 框架，以 Wordpress 和 Joomla 为主，尤其是 Wordpress，占比高达 57%。

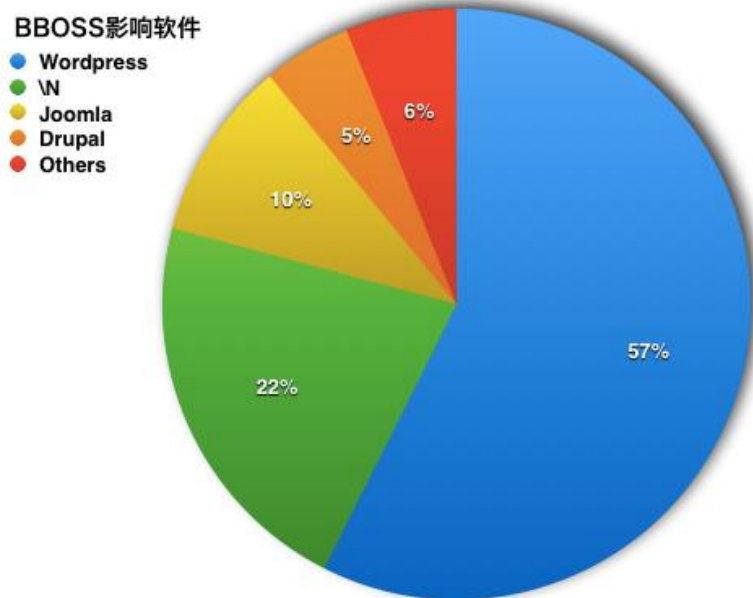


图 7-1 BBOSS 影响软件比例（\N 表示无任何 CMS 软件）

控制超过 12 万的网站，BBOSS 背后的技术体系也极其完善，可以看到该组织为了更高效掌控和易隐藏，使用了多层架构，认为其具有控制超大规模集群肉鸡网站的能力。

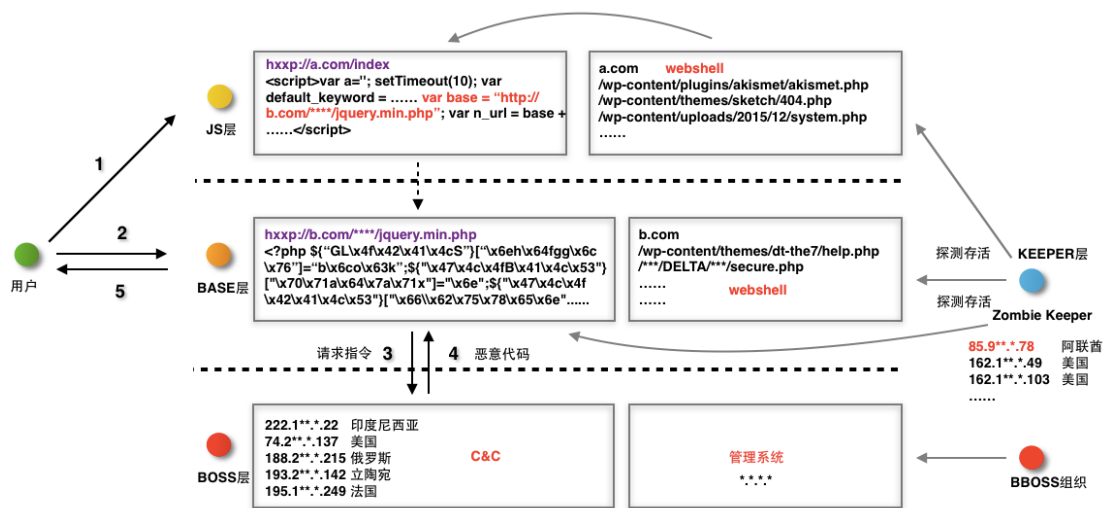


图 7-2 BBOSS 系统技术体系

BBOSS 技术体系中，大致分为 4 层，分别是 JS 层，BASE 层，KEEPER 层和 BOSS 层。每一层的肉鸡分工明确，配合密切。JS 层为直接接触用户的站点，页面中嵌入了 js，构造请求转发流量到 BASE 层。BASE 层会向 BOSS 层请求指令，完成校验后 BOSS 层根据当前需要进行的攻击返回攻击指令，再由 BASE 层下发给用户。同时，KEEPER 层会定期对 JS 层和 BASE 层站点进行探测存活、增删修改、漏洞利用等操作。

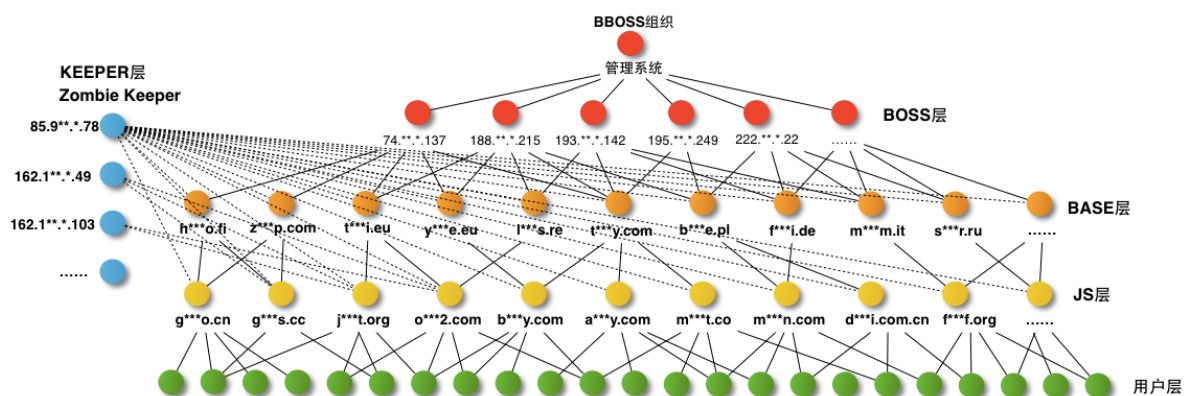


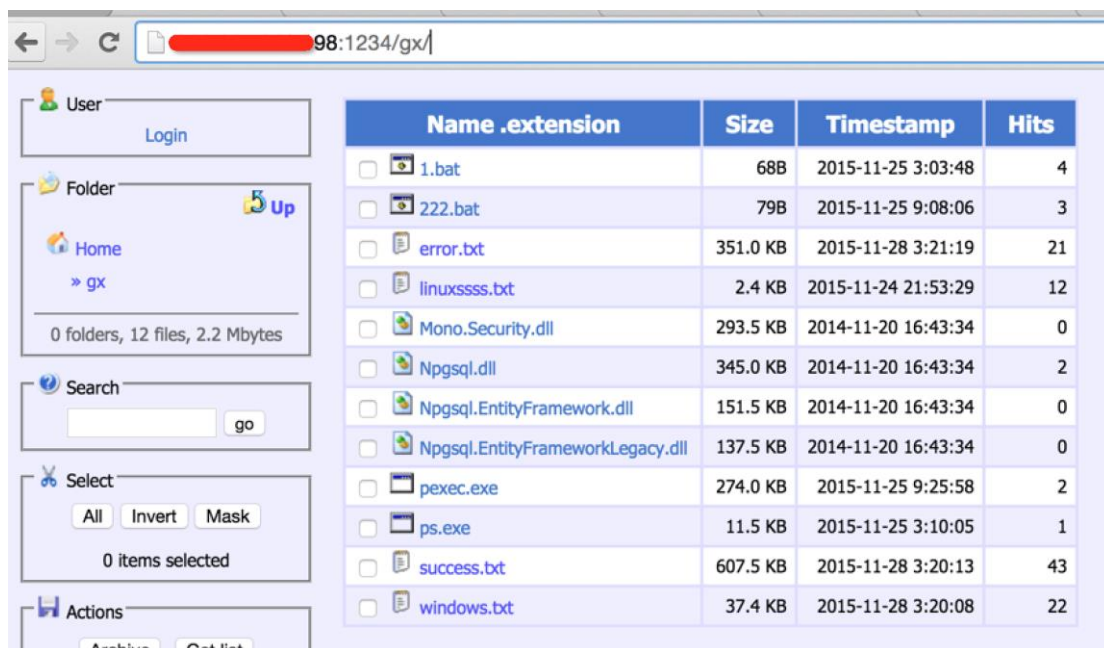
图 7-3 BBOSS 分层关系

研究人员分析攻击者处于 GMT+5 时区，其肉鸡遍布各个国家，主要用来进行勒索软件的植入和恶意推广。BBOSS 技术架构体系高度成熟，多级分层，代码都经过混淆，有很强的攻防对抗意识。

7.2 PostgreSQL 弱口令致使数千台服务器沦陷

PostgreSQL 与 MySQL 类似，属于关系型数据库的一种，但用户量远不及 MySQL 多，所以很少在常见的黑客教程中被提及。不过，云盾态势感知通过分析异常流量中的蛛丝马迹，成功捕获到一起利用 PostgreSQL 弱口令批量植入木马的事件。

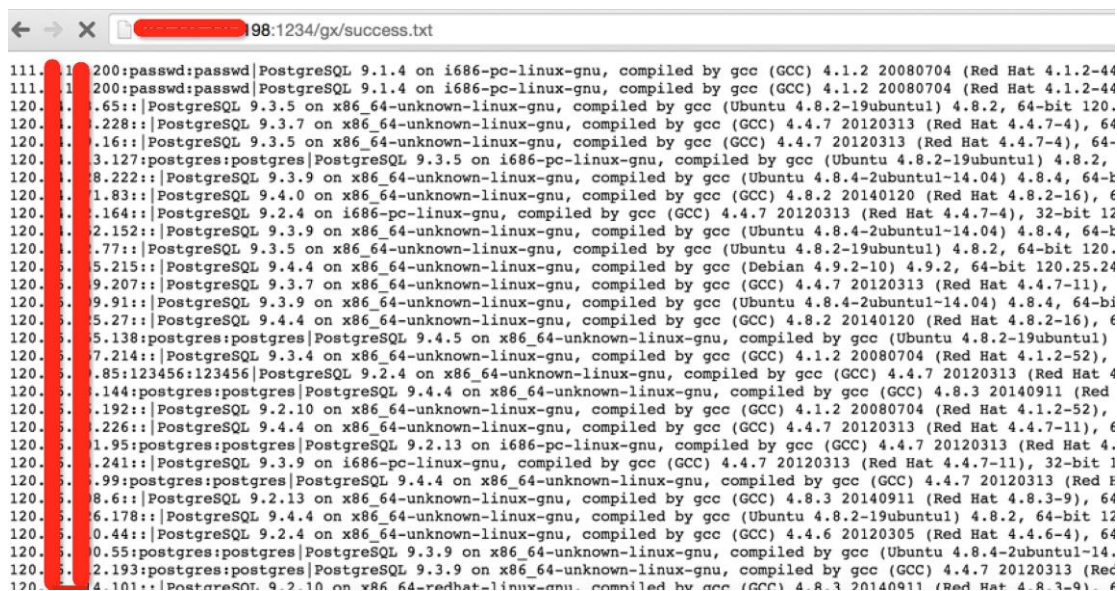
2015 年 11 月 27 日星期五，云盾态势感知系统产出了一条异常的告警，研究人员顺藤摸瓜找到了一个传播恶意文件的 HFS 服务器。



在 HFS 服务器中，发现了黑客用来批量扫描漏洞和自动攻击的程序：
ps.exe 和 pexec.exe。下载到本地进行分析之后，判定此工具为针对
PostgreSQL 数据库的自动化攻击程序。

[illegible]

分析其它文件，我们还找到了攻击者已经扫描到的 PostgreSQL 弱口令和利用成功的 IP 列表：



```
111.111.111.200:passwd:passwd|PostgreSQL 9.1.4 on i686-pc-linux-gnu, compiled by gcc (GCC) 4.1.2 20080704 (Red Hat 4.1.2-44)
111.111.111.200:passwd:passwd|PostgreSQL 9.1.4 on i686-pc-linux-gnu, compiled by gcc (GCC) 4.1.2 20080704 (Red Hat 4.1.2-44)
120.155.165::|PostgreSQL 9.3.5 on x86_64-unknown-linux-gnu, compiled by gcc (Ubuntu 4.8.2-19ubuntu1) 4.8.2, 64-bit 120.
120.155.228::|PostgreSQL 9.3.7 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.4.7 20120313 (Red Hat 4.4.7-4), 64
120.155.116::|PostgreSQL 9.3.5 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.4.7 20120313 (Red Hat 4.4.7-4), 64-
120.155.13.127:postgres:postgres|PostgreSQL 9.3.5 on i686-pc-linux-gnu, compiled by gcc (Ubuntu 4.8.2-19ubuntu1) 4.8.2,
120.155.18.222::|PostgreSQL 9.3.9 on x86_64-unknown-linux-gnu, compiled by gcc (Ubuntu 4.8.4-2ubuntu1-14.04) 4.8.4, 64-b
120.155.1.83::|PostgreSQL 9.4.0 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.8.2 20140120 (Red Hat 4.8.2-16), 6
120.155.1.164::|PostgreSQL 9.2.4 on i686-pc-linux-gnu, compiled by gcc (GCC) 4.4.7 20120313 (Red Hat 4.4.7-4), 32-bit 12
120.155.12.152::|PostgreSQL 9.3.9 on x86_64-unknown-linux-gnu, compiled by gcc (Ubuntu 4.8.4-2ubuntu1-14.04) 4.8.4, 64-b
120.155.1.77::|PostgreSQL 9.3.5 on x86_64-unknown-linux-gnu, compiled by gcc (Ubuntu 4.8.2-19ubuntu1) 4.8.2, 64-bit 120.
120.155.15.215::|PostgreSQL 9.4.4 on x86_64-unknown-linux-gnu, compiled by gcc (Debian 4.9.2-10) 4.9.2, 64-bit 120.25.24
120.155.19.207::|PostgreSQL 9.3.7 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.4.7 20120313 (Red Hat 4.4.7-11),
120.155.19.91::|PostgreSQL 9.3.9 on x86_64-unknown-linux-gnu, compiled by gcc (Ubuntu 4.8.4-2ubuntu1-14.04) 4.8.4, 64-bi
120.155.15.27::|PostgreSQL 9.4.4 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.8.2 20140120 (Red Hat 4.8.2-16), 6
120.155.15.138:postgres:postgres|PostgreSQL 9.4.5 on x86_64-unknown-linux-gnu, compiled by gcc (Ubuntu 4.8.2-19ubuntu1)
120.155.17.214::|PostgreSQL 9.3.4 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.1.2 20080704 (Red Hat 4.1.2-52),
120.155.18.5:123456:123456|PostgreSQL 9.2.4 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.4.7 20120313 (Red Hat 4
120.155.17.144:postgres:postgres|PostgreSQL 9.4.4 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.8.3 20140911 (Red
120.155.1.192::|PostgreSQL 9.2.10 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.1.2 20080704 (Red Hat 4.1.2-52),
120.155.1.226::|PostgreSQL 9.4.4 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.4.7 20120313 (Red Hat 4.4.7-11), 6
120.155.1.195:postgres:postgres|PostgreSQL 9.2.13 on i686-pc-linux-gnu, compiled by gcc (GCC) 4.4.7 20120313 (Red Hat 4.
120.155.1.241::|PostgreSQL 9.3.9 on i686-pc-linux-gnu, compiled by gcc (GCC) 4.4.7 20120313 (Red Hat 4.4.7-11), 32-bit 1
120.155.19.99:postgres:postgres|PostgreSQL 9.4.4 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.4.7 20120313 (Red
120.155.18.6::|PostgreSQL 9.2.13 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.8.3 20140911 (Red Hat 4.8.3-9), 64
120.155.16.178::|PostgreSQL 9.4.4 on x86_64-unknown-linux-gnu, compiled by gcc (Ubuntu 4.8.2-19ubuntu1) 4.8.2, 64-bit 12
120.155.10.44::|PostgreSQL 9.2.4 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.4.6 20120305 (Red Hat 4.4.6-4), 64
120.155.10.55:postgres:postgres|PostgreSQL 9.3.9 on x86_64-unknown-linux-gnu, compiled by gcc (Ubuntu 4.8.4-2ubuntu1-14.
120.155.12.193:postgres:postgres|PostgreSQL 9.3.9 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.4.7 20120313 (Red
120.155.14.101::|PostgreSQL 9.2.10 on x86_64-unknown-linux-gnu, compiled by gcc (GCC) 4.8.3 20140911 (Red Hat 4.8.3-9), 6
```

图 7-6 攻击者服务器上的 IP 列表

对这些 IP 进行了简单的分析统计，发现已经有数千台服务器被植入木马，已然是一个数量可观的僵尸网络。

7.3 黄赌毒挂马事件

黑色产业愈发猖獗，黑客攻击自动化、规模化越来越明显。在 2015 年 8 月捕获的一次批量植入赌博色情挂马的事件中，阿里云安全团队在定位到的攻击源上发现了整套的自动化扫描 Webshell、插入挂马页面并提交搜索引擎爬取的自动化攻击系统，通过该系统自动对挂马 URL 分类、打标，统一管理。经过统计，该攻击源仅 3 个月挂马的 URL 就有 62 万条，影响的 web 应用主要为 DedeCMS、phpweb、良精南方等。

<div> <div>导入向导</div> <div>导出向导</div> <div>筛选向导</div> <div>网格查看</div> <div>表单查看</div> <div>备注</div> <div>十六进制</div> <div>图像</div> <div>升序排序</div> <div>降序排序</div> <div>移除排序</div> </div>						
ID	Site	Url	LocalFile	Type	Upload_Time	
609280	www. [REDACTED] .com	http://www. [REDACTED] .com/fuzell/w88/index.php	D:/业务管理/data/smallsystem/php	在线版-w88	2015-07-29	
609279	www. [REDACTED] .com	http://www. [REDACTED] .com/gewei00/w88/index.php	D:/业务管理/data/smallsystem/php	在线版-w88	2015-07-29	
609278	www. [REDACTED] .com	http://www. [REDACTED] .com/xiawu55/w88/index.php	D:/业务管理/data/smallsystem/php	在线版-w88	2015-07-29	
609277	www. [REDACTED] .com	http://www. [REDACTED] .com/muqian33/w88/index.php	D:/业务管理/data/smallsystem/php	在线版-w88	2015-07-29	
609276	www. [REDACTED] .com	http://www. [REDACTED] .com/fuzell/yzc/index.php	D:/业务管理/data/smallsystem/php	在线版-ycz	2015-07-29	
609275	www. [REDACTED] .com	http://www. [REDACTED] .com/muqian33/w88/index.php	D:/业务管理/data/smallsystem/php	在线版-w88	2015-07-29	
609274	www. [REDACTED] .com	http://www. [REDACTED] .com/jianyu22/w88/index.php	D:/业务管理/data/smallsystem/php	在线版-w88	2015-07-29	
609273	www. [REDACTED] .com	http://www. [REDACTED] .com/gewei00/yzc/index.php	D:/业务管理/data/smallsystem/php	在线版-ycz	2015-07-29	
609272	www. [REDACTED] .com	http://www. [REDACTED] .com/fuzell/w88/index.php	D:/业务管理/data/smallsystem/php	在线版-w88	2015-07-29	
609271	www. [REDACTED] .com	http://www. [REDACTED] .com/gewei00/w88/index.php	D:/业务管理/data/smallsystem/php	在线版-w88	2015-07-29	
609270	www. [REDACTED] .com	http://www. [REDACTED] .com/xiawu55/yzc/index.php	D:/业务管理/data/smallsystem/php	在线版-ycz	2015-07-29	
609269	www. [REDACTED] .cn	http://www. [REDACTED] .cn/xiawu55/yzc/index.php	D:/业务管理/data/smallsystem/php	在线版-ycz	2015-07-29	
609268	www. [REDACTED] .com	http://www. [REDACTED] .com/fuzell/yzc/index.php	D:/业务管理/data/smallsystem/php	在线版-ycz	2015-07-29	
609267	www. [REDACTED] .com	http://www. [REDACTED] .com/muqian33/yzc/index.php	D:/业务管理/data/smallsystem/php	在线版-ycz	2015-07-29	
609266	www. [REDACTED] .com	http://www. [REDACTED] .com/gewei00/yzc/index.php	D:/业务管理/data/smallsystem/php	在线版-ycz	2015-07-29	
609265	www. [REDACTED] .com	http://www. [REDACTED] .com/xiawu55/w88/index.php	D:/业务管理/data/smallsystem/php	在线版-w88	2015-07-29	
609264	www. [REDACTED] .com	http://www. [REDACTED] .com/jianyu22/yzc/index.php	D:/业务管理/data/smallsystem/php	在线版-ycz	2015-07-29	
609263	www. [REDACTED] .cn	http://www. [REDACTED] .cn/muqian33/yzc/index.php	D:/业务管理/data/smallsystem/php	在线版-ycz	2015-07-29	
609262	www. [REDACTED] .cn	http://www. [REDACTED] .cn/jianyu22/yzc/index.php	D:/业务管理/data/smallsystem/php	在线版-ycz	2015-07-29	
609261	www. [REDACTED] .com	http://www. [REDACTED] .com/fuzell/w88/index.php	D:/业务管理/data/smallsystem/php	在线版-w88	2015-07-29	

图 7-7 黑客自动化挂马系统数据库

PART EIGHT

总结

8 总结

随着云计算技术不断发展，未来几年中，将会有越来越多的网站运行在“云”中，云端安全也将迎来一个新的局面。

Web 攻击越演越烈，全网知识库大大丰富，建站系统漏洞被广泛利用，新漏洞发现与利用的速度越来越快，以及第三方代码托管平台被攻击，种种迹象表明网络攻击在 2016 年会大大增加。

DT 时代，传统以阻断和防御为核心的安全策略已经不再适合瞬息万变的互联网和云计算安全发展，信息安全的实现正在演变为一个大数据分析问题，大规模的安全数据需要被有效地关联、分析和挖掘才能探寻出真正的威胁。通过机器学习的方法进行自动侦测异常行为，通过大数据技术来提高扩展性、灵活性以及处理性能，最终让企业用户减少处理繁缛的数据源、规则和事件的成本，让 IT 部门用最少的人完成更多的事。



附录

附录：2015 年全球十大网络安全事件

阿里云安全团队从影响范围、破坏程度、标志性意义等维度出发，评选出 2015 年十大网络安全事件。

时间	事件	上榜理由
2015.12	Juniper 防火墙和安全服务网关等设备存在“非授权代码”。	允许入侵者远程获得管理员访问权限。Juniper 设备本身就是安全系统，这个漏洞具有重要的现实意义。
2015.11	ISIS Twitter 账号被盗取，Anonymous 宣称已获得 5500 个支持 ISIS 的 Twitter 账号的控制权。	Twitter 账号争夺战的再次上演。账号安全的重要性再次显现出来，与用户安全意识的提升密切相关。
2015.11	一个自称 Armada Collective 的黑客组织以 DDoS 攻击威胁敲诈加密电子邮件服务商 Protomail。Protomail 公司屈服，并支付 15 比特币（6000 美金）。	一方面，这是一起非常具有代表性的网络敲诈勒索事件，另一方面，从结果来看，Protomail 支付款项后仍旧遭到攻击更说明问题。
2015.9	希尔顿酒店及其连锁机构的 PoS 系统被入侵，可能导致大量用户私密信息（如信用卡）泄露。	PoS 系统是一个关键的攻防点。黑客通过 PoS 入侵系统的事件屡有发生。
2015.9	卡巴斯基发布研究报告揭露一个基于卫星 C&C 机制的 APT 组织——Turla。	顶尖黑客组织，由于卫星的 Internet 覆盖区广泛以及可能因劫持卫星通信引发的风险，后果不堪设想。
2015.9	“火眼”研究人员称发现来自朝鲜的黑客利用 Hangul 软件的 0day 漏洞入侵韩国的政府系统。	典型的 APT 攻击，利用目标特定应用的 0day 漏洞。
2015.7	“火眼”研究人员发现俄罗斯黑客针对美国防部联合参谋部的入侵行为，致使其电邮系统关闭近两周，影响 4000 人。	又一起典型的鱼叉式钓鱼邮件攻击，恶意代码 HAMMERTOSS 绕过了美国防部所有的防御系统。

2015.6	卡巴斯基确认入侵卡巴斯基内网和入侵伊朗核问题“六方”会谈酒店的是超级计算机病毒 Duqu 2.0，采用了富士康公司合法数字证书。	一个开发成本高达 5000 万美元的恶意软件，一个成功入侵全球安全技术顶尖公司的内网的恶意软件。
2015.3	代码托管网站 GitHub 遭遇大流量 DDoS 攻击，攻击时长超过 100 小时，攻击者劫持 JS 脚本并将其替换成恶意代码。	来自 JS 代码的 DDoS 攻击，无论从攻击手段还是攻击时长上来看，对于 DDoS 攻击来说均是一个里程碑。
2015.1	第二大医疗保险公司 Anthem 遭黑客入侵，近 8000 万用户数据泄露。	从用户信息泄露事件角度上来说，Anthem 用户信息泄露的数量超过了 Target 7000 万用户信息和 HomeDepot 的 5600 万用户信息，是 2015 年 No.1 的用户信息失窃案。

2015 年十大网络安全事件

关于阿里云云盾

阿里云云盾是阿里巴巴集团多年来安全技术研究积累的成果，结合阿里云云计算平台强大的数据分析能力，为互联网用户提供DDoS防护、CC攻击防护、云服务器入侵防护、WEB攻击防护、弱点分析、安全态势感知、渗透测试、信息内容安全检测及管控等一站式安全服务，帮助互联网用户轻松应对各种攻击、安全漏洞问题，确保云服务稳定正常。

联系我们

官方微博

新浪微博：阿里云 阿里云安全

官方微信

微信公众号：阿里云 阿里云安全



网站：<https://www.aliyun.com/product/sas>