威胁情报新应用：量化信息安全风险

赵毅 2016.6.23

GooAnn gooann.com 谷安天下

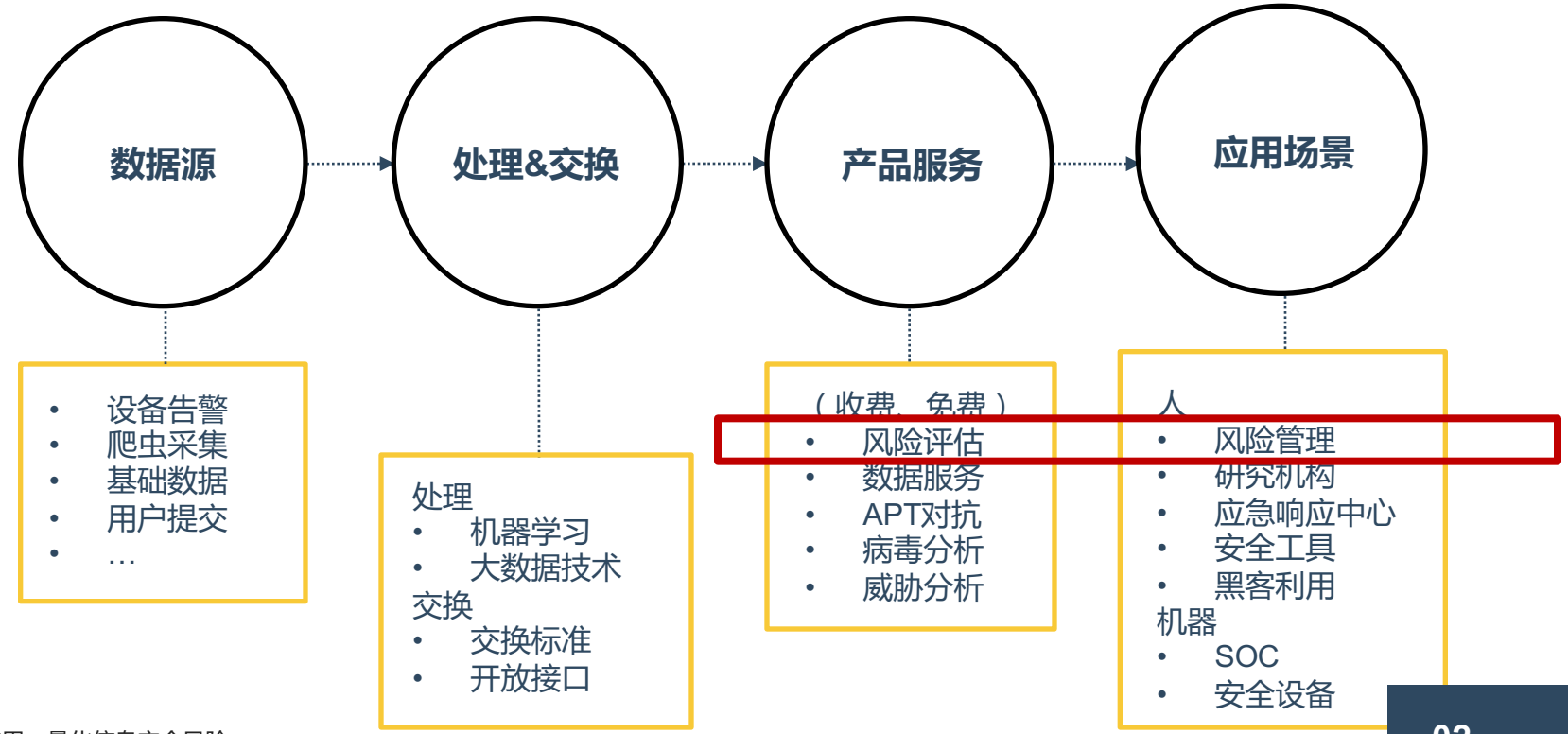
优秀的数据资源

abuse.ch,alienvault OTX,antispam.imp.ch,anva
autoshun.org,bambenekconsulting.com,ciarmy.
com,clean-mx.de,Crowdstrike,CyberUnited
dell secureworks,dragonresearchgroup.org
dyndns.org,eCrime eXchange Fackbook,
emergingthreats.net,FireEye/Mandiant,IBM-
xforce,infiltrated.net,ISACs / US-CERT
isc.sans.edu,joewein.net,malwaredomainlist.co
m, malwaredomains.com,malwaregroup.com
malwaremustdie.org,manitu.net,MAPP,McAfee
Threat Intelligence,montanamenagerie.org,
MUTE,Norse IPViking/Darklist,nosec.org,
nothink.org,openbl.org,OpenDNS,OSINT,
packetmail.net,Palo Alto Wildfire,phishtank
projecthoneypot.org,qbox.me,Qihoo 360,
RecordedFuture,RSA netwitness live/verisign
idefense, rulez.sk,spamhaus.org,surriel.com,
symantec deepsight,Team Cymru,Teamcymru,
the-haleys.com,threatbook.cn,ThreatStream,
url blocklist,virbl.org,Virustotal,Vorstack

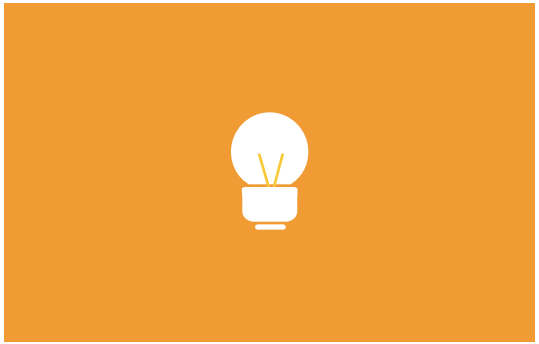
威胁情报标准

- STIX - Structured Threat Information eXpression
- TAXII - Trusted Automated eXchange of Indicator Information
- CybOX - Cyber Observable eXpression
- MAEC - Malware Attribute Enumeration and Characterization
- OpenIOC - Open sourced schema from Mandiant
- IODEF - Incident Object Description Exchange Format
- CIF - Collective Intelligence Framework
- IDXWG - Incident Data eXchange Working Group

威胁情报产业


数据源
处理&交换
产品服务
应用场景
• 设备告警
• 爬虫采集
• 基础数据
• 用户提交
• …
处理
• 机器学习
• 大数据技术
交换
• 交换标准
• 开放接口
（收费、免费）
• 风险评估
• 数据服务
• APT对抗
• 病毒分析
• 威胁分析
人
• 风险管理
• 研究机构
• 应急响应中心
• 安全工具
• 黑客利用
机器
• SOC
• 安全设备

主要内容



3个问题

3个价值

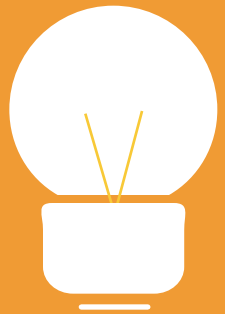
3个案例

三个问题
Three questions

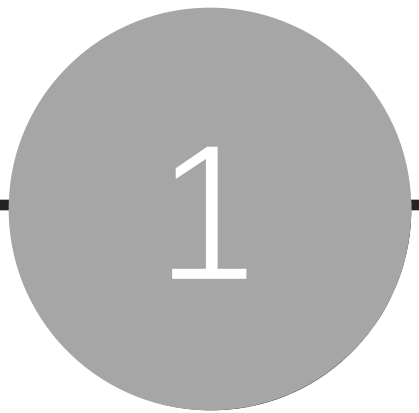
互联网 + ？，有哪些未知的资产和风险？

你的企业安全水平在行业中处于什么位置？

合作伙伴、供应商带来的第三方安全风险如何管理？



三个案例
Three cases



新视角看风险，应对安全事件。

威胁情报大数据赋予了新视角的能力

钓鱼网站现状

2016年1月至5月钓鱼网站

月份	数量
2016年1月	16560
2016年2月	14943
2016年3月	19118
2016年4月	17762
2016年5月	15617
总数	84000

2016年银行业钓鱼网站TOP10

机构	数量
建设银行	33575
工商银行	30241
招商银行	8037
农业银行	1118
交通银行	823
中国银行	304
平安银行	157
广发银行	100
中国邮政	57
民生银行	37

2016年证券业钓鱼网站TOP10

机构	数量
海通证券	456
招商证券	368
华泰证券	300
国泰君安证券	276
中信证券	258
中国银河证券	235
光大证券	231
广发证券	215
东方证券	183
国信证券	162

黑名单的影响

MOil 企业邮箱 垃圾邮件隔离提醒

您好：

您有2封新邮件被系统识别为垃圾邮件，已被自动隔离，摘要信息见下表。

发件人	主题	日期	找回
hengzhi.dm@sailmail....	"【紫荆教育 MBA】国内...	2016/03/17	移回收件箱
"Prezi" <email@email....	A fresh Prezi template t...	2016/03/16	移回收件箱

不再收取该垃圾邮件隔离提醒，可点此 不再收取此类邮件
重新收取此类邮件请到邮箱中[设置]-[客户端设置]开启

2014-05-25 11:28:48 H=(21cn.com) [183.56.131.105]:7545 F=rejected RCPT: "JunkMail rejected - (21cn.com) [183.56.131.105]:7545 is in an RBL, see IP 183.56.131.105 is UCEPROTECT-Level 1 listed. See http://www.uceprotect.net/rblcheck.php?ipr=183.56.131.105"

整合全球顶尖威胁情报资源

全球 100+威胁情报数据资源，利用大数据挖掘分析方法，对实时情报数据进行风险分析，每天量化计算风险，提升风险管理能力。

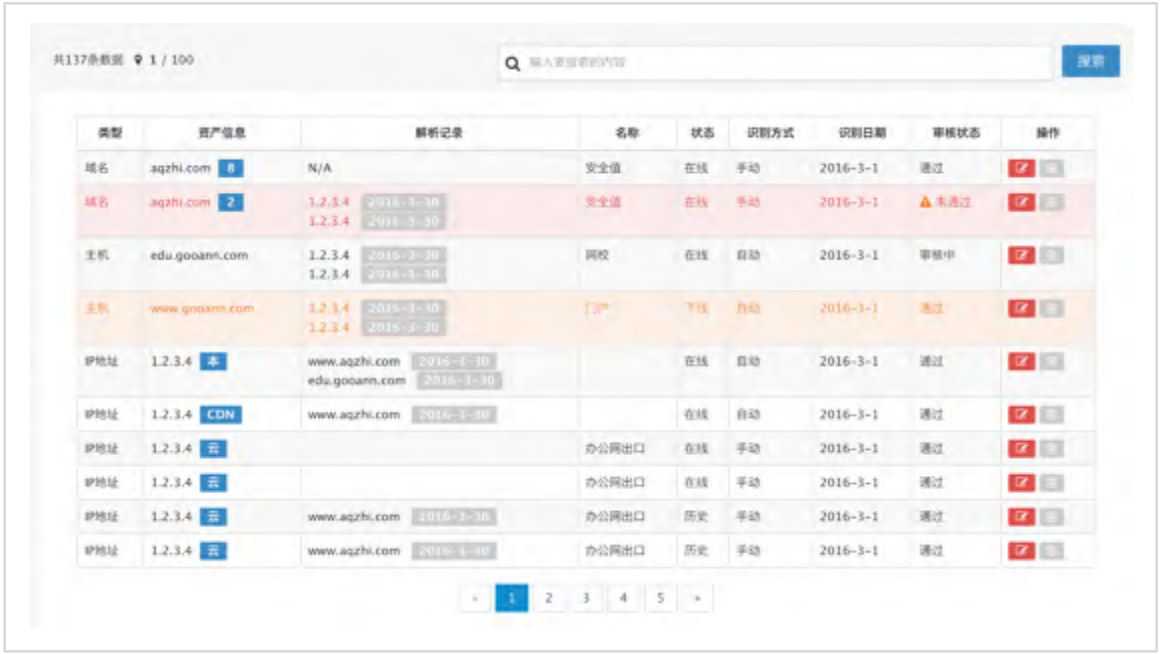
全球威胁情报数据源 + 实时互联网通信数据 + 全面互联网基础数据

价值一：基于外部数据进行风险评估

基于外部数据识别未知资产

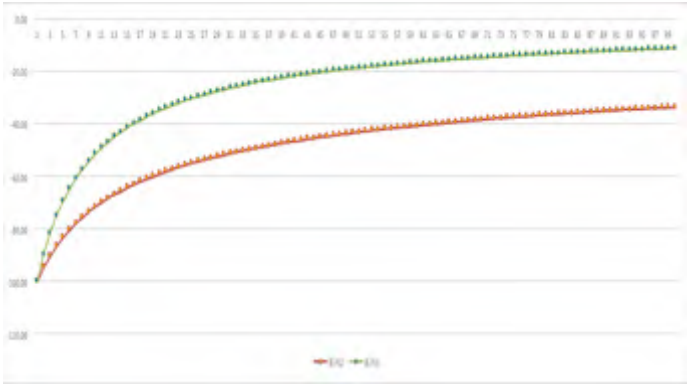
通过数据关联可以识别互联网上活动的资产。

- **域名**：相同主体注册的域名
- **主机**：面向互联网开放的各种服务，包括Web、Mail、FTP、API等一切可以访问的应用
- **IP地址**：公网出入口的IP地址，包括系统入口、办公网出口、第三方的CDN或者云服务



全新视角揭示风险，多维度安全评估

量化安全风险，实现风险管理常态化



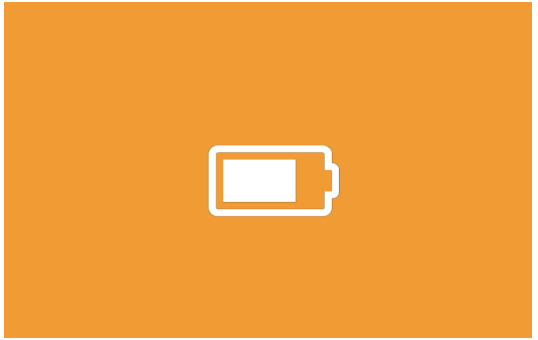
价值一：基于外部数据进行风险评估

新视角，新风险

建立大数据量化风险评估模型，从外部全新视角识别企业未知风险，让企业对互联网风险一目了然。

实时数据，常态管理

对全球 100+ 个威胁情报资源实时数据进行查询，每天进行风险识别和分析，掌握与企业相关的威胁情报。



定量化分析

用数据说话，量化安全风险，以数字表示安全状态，让安全风险更清晰可见、更容易管理。

三个案例
Three cases

2

3

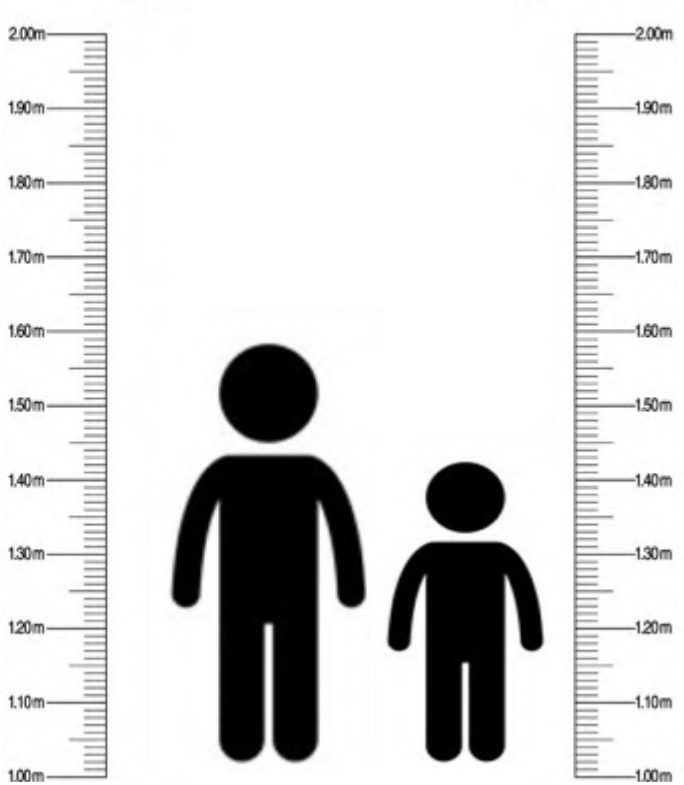
新视角看风险，应对安全事件。

建立信息安全量化评价体系，分析行业安全趋势

价值二：行业安全趋势分析和差距对比

价值二：统一的风险评价标准

建立统一、可测量的量化风险评价标准



价值二：分析行业安全值报告

对行业单位进行数据采集，基于威胁情报数据，结合大数据技术跟踪各行业安全趋势形成行业报告。

https://www.aqzhi.com/themes/default/assets/link/finance_industry_2016.Q1.pdf

行业安全值（2016-6-7）

银行业 808	证券业 878	保险业 853	卫生 817	教育 683	互联网金融 857
物流	制造	房地产	能源	电子商务与零售业	交通运输

报告概述

安全值行业报告是基于威胁情报数据，利用大数据的分析方法对行业整体安全状态进行评价和分析，本报告对互联网金融行业中 336 家互联网金融公司进行安全评价和量化风险分析。

本报告是针对各互联网金融公司的数据信息进行采集，共计 336 家公司的安全值进行分析，包括第三方支付 44 家、P2P 公司 150 家、众筹 110 家、消费金融 32 家，并从业务安全、隐私安全、应用安全、主机安全、网络安全、环境安全 6 个维度进行风险量化分析。

通过安全值对行业第一季度的数据分析发现：

根据 2016-5-4 安全值数据，互联网金融行业安全值为 857，整体评价为“一般”，共 336 个公司，其中 182 家（54%）评价为“良好”；99 家（30%）评价为“一般”；55 家（16%）评价为“较差”。

隐私安全问题较为普遍，336 家机构中 288 家存在该风险，约 86%，主要是域名未进行隐私保护问题较多，属于影响范围大，但影响程度一般的情况，336 家机构中有 288 家（86%）的域名未做隐私保护，存在域名信息泄露风险，构成了隐私安全的主要问题，1097 个域名没有申请域名隐私保护，通过 Whois 可以查询域名注册信息。

其次是应用安全和网络安全问题，在 336 家中有 140 家存在应用安全风险，约占 42%，主要问题是第三方漏洞平台上被发布安全漏洞和经常受到 Web 攻击，其中有 134 家机构（40%）被公开披露了安全漏洞，构成了应用安全威胁的主要问题，近 90 天内共发现 208 条第三方安全社区上的安全漏洞记录，平均每个公司 30 天内被披露 1.5 个漏洞。

336 家机构中有 111 家（33%）公司存在僵尸网络的风险，90 天内共有 55 个 IP 网络受到影响，共发现 2381 条对外的非法攻击请求。

Copyright ©2016 安全值. All Rights Reserved.

1. 行业总体概况

根据 2016-5-4 安全值数据，互联网金融行业安全值为 857，整体评价为“一般”，共 336 个公司，其中 182 家（54%）评价为“良好”；99 家（30%）评价为“一般”；55 家（16%）评价为“较差”。

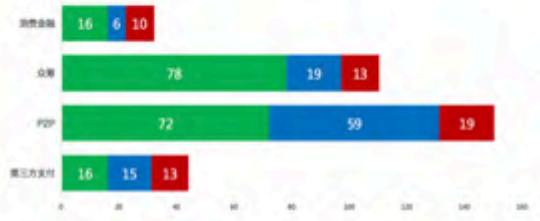
评价	得分范围	单位数量	占比
良好	901-1000	182	54%
一般	601-900	99	30%
较差	600-600	55	16%

1.1. 总体安全值分布

从安全值的分布情况来看，其中 211 家机构得分高于或等于平均值 857，125 家机构得分低于平均值，安全值得分分布大多数集中在良好的状态，平均分数线主要被过低的得分公司影响，最低分数为 339 分。

Copyright ©2016 安全值. All Rights Reserved.

1.2. 按照业务分类统计



	平均值	机构数量	良好	一般	较差
第三方支付	780	44	16	15	13
P2P	853	150	72	59	19
众筹	902	110	78	19	13
消费金融	829	32	16	6	10

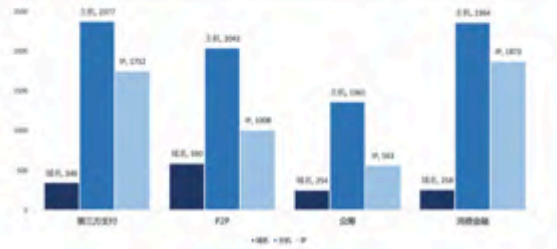
根据业务类型分类，P2P 公司数量最多，150 家机构中“一般”和“较差”水平的有 78 家，占城商行的 52%，平均安全值为 853 分；

众筹公司的平均安全值最高 902 分，110 家机构中“一般”和“较差”水平的有 32 家，仅占众筹公司的 29%。

1.3. 互联网资产统计

安全值对互联网资产进行分析统计，包括各机构注册的域名、面向互联网开放的主机服务（不仅限于 Web 服务的网站）和公网 IP 地址。

Copyright ©2016 安全信. All Rights Reserved.



	域名数量	主机数量	IP 数量	平均每机构资产数量
第三方支付	346	2377	1752	102
P2P	590	2042	1008	24
众筹	254	1361	563	20
消费金融	258	2364	1873	140
总体	1448	8144	5196	44

44 家第三方支付公司的资产数量较多，同时面临的风险最大，根据对互联网开放的域名、主机和 IP 地址统计，第三方支付公司域名共有 346 个，公网主机 2377 个，公网 IP 地址 1752 个，平均每个机构有 102 个互联网资产，安全值平均得分 780。

2. 风险分布及量化评估

根据业内的信息安全风险管理最佳实践，结合风险等级、影响范围、频率、数量、时间各方面要素建立量化风险的计算模型，对整体情况的 6 个风险域（业务安全、应用安全、隐私安全、主机安全、网络安全和环境安全）进行量化评价，综合来看隐私安全问题普遍存在，其次是应用安全和网络安全方面。

Copyright ©2016 安全信. All Rights Reserved.

威胁情报新
9

	机构数量	业务安全	应用安全	隐私安全	主机安全	网络安全	环境安全
第三方支付	44	31	24	44	33	15	0
P2P	150	58	77	127	75	86	0
众筹	110	26	22	91	37	23	0
消费金融	32	17	17	26	19	14	0
总计	336	132	140	288	164	138	0

通过安全值对互联网金融行业第一季度的数据分析发现：

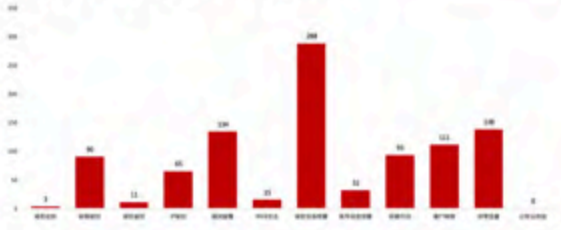
1. 隐私安全问题较为普遍，336 家机构中 288 家存在该风险，约 86%，主要是域名未进行隐私保护问题较多，该风险影响范围大，但影响程度一般，风险详细分析见 3.3 章。
2. 其次是应用安全和主机安全问题，在 336 家中有 140 家存在应用安全风险，约占 42%，主要问题是第三方漏洞平台上被发布安全漏洞，336 家机构中有 111 家（33%）

Copyright ©2016 安全值. All Rights Reserved.

公司存在僵尸网络的风险，风险详情见 3.1 章和 3.2 章。

3. 主要风险详细分析

安全值整体基于 12 个风险指标支撑 6 个维度的安全评价，分别对各项风险指标影响的机构数量进行统计便于找出较集中的问题。



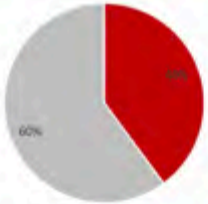
	域名劫持	后台被入侵	域名被封	IP被封	漏洞披露	WEB攻击	域名信息披露	账号信息泄露	恶意代码	僵尸网络	异常流量	公有云风险
第三方支付	0	28	5	12	24	1	44	20	29	19	15	0
P2P	2	37	3	27	75	6	127	8	39	50	86	0
众筹	0	10	1	18	18	5	91	1	10	31	23	0
消费金融	1	15	2	8	17	3	26	3	15	11	14	0
总体	**3**	**90**	**11**	**65**	**134**	**15**	**288**	**32**	**93**	**111**	**138**	**0**

3.1. 漏洞披露风险分析

互联网安全社区上公开披露的安全漏洞应该优先处理，避免漏洞在修复之前被公开，引来恶意攻击和影响形象，应通过安全顾问的帮助分析问题的根源，避免同类漏洞的产生。

Copyright ©2016 安全值. All Rights Reserved.

漏洞披露



336 家中有 134 家机构（40%）被公开披露了安全漏洞，构成了应用安全威胁的主要问题。

近 90 天内共发现 208 条第三方安全社区上的安全漏洞记录，平均每个公司 30 天内被披露 1.5 个漏洞。

[redacted]	设计缺陷可刷单	2016-05-03
[redacted]	邮箱弱口令泄露未来技术规划涉及用户手	2016-05-03
[redacted]	简单单通用存储型xss	2016-05-03
[redacted]	系统tomcat配置不当可getshell	2016-04-29
[redacted]	app几种安全问题	2016-04-28
[redacted]	ndroid客户端远程命令执行	2016-04-28
[redacted]	远程命令执行漏洞	2016-04-28
[redacted]	SQL注射漏洞	2016-04-28
[redacted]	站配置不当导致getshell可威胁内网	2016-04-28
[redacted]	重要系统任意密码重置	2016-04-28
[redacted]	存在SQL注入	2016-04-27
[redacted]	漏洞泄露敏感信息(cookie\电话\名字\身份证	2016-04-27
[redacted]	处注入	2016-04-27
[redacted]	处注入	2016-04-27
[redacted]	xss	2016-04-27

处置建议：

1. 及时与第三方漏洞平台取得联系，认领安全漏洞，并进行漏洞修补；
2. 对漏洞修补后的效果进行验证；
3. 对所有系统全面进行安全漏洞检查和渗透测试，对漏洞进行分类管理，跟踪漏洞处置过程和结果，完善上线安全测试工作，保证信息系统无高、中危的安全漏洞。

3.2. 僵尸网络风险分析

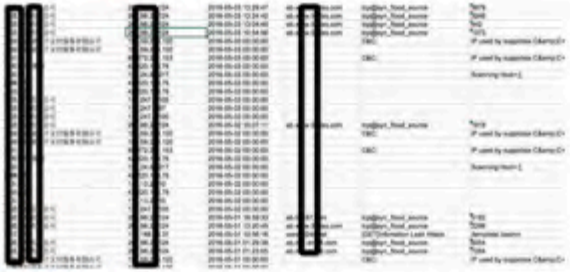
网络内的服务器或者终端已经被植入木马、后门，被非法控制成为“肉鸡”，对外发起了扫描或者攻击的行为。

Copyright ©2016 安全信. All Rights Reserved.

僵尸网络

336 家机构中有 111 家（33%）公司存在僵尸网络的风险。

90 天内共有 55 个 IP 网络受到影响，共发现 2381 条对外的非法攻击请求。



处置建议：

1. 分析僵尸网络地址对应网络，如果是服务器网络则需要对系统进行全面的风险评估；
2. 如果僵尸网络地址对应办公网，需通过出口路由器日志定位终端主机，并检查木马、后门，加强终端安全保护；
3. 加强终端使用安全管理，上网行为管理。

3.3. 域名信息泄露风险分析

在注册商成功注册域名后，你的姓名、联系地址、电话、Email 等注册信息将被存储到域名 whois 信息数据库中，任何人都可公开查询到这些信息，隐私无法保障。

Copyright ©2016 安全信. All Rights Reserved.

三个案例
Three cases

新视角看风险，应对安全事件。

建立信息安全量化评价体系，分析行业安全趋势

3

合作伙伴、供应商带来的第三方风险

价值三：第三方安全风险评估

第三方安全风险管理的必要性

大多数公司忽略了潜伏在他们的合作伙伴中的安全风险。在2015年的网络犯罪报告,普华永道发现,只有16%的受访者表示,他们不止一次评估第三方的安全—23%不评估第三方。合作伙伴和供应商的安全风险不容忽视，这已经成为国内外所关注的一个主要风险领域。

http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf

行业对信息科技外包风险的要求

《银行业金融机构信息科技外包风险监管指引》

- 银行业金融机构应当特别加强对具有机构集中度特点的外包服务提供商的财务、内控、安全管理情况的持续监控，建立信息收集机制，及时掌握风险事件情况。
- 定期对服务提供商进行安全检查，获取服务提供商自评估或第三方评估报告。
- 银行业金融机构对关联外包服务提供商定期进行的安全检查，不得以服务提供商的自评估替代，不得因关联关系而影响检查的独立性、客观性及公正性。

总结：基于威胁情报数据的量化风险管理

利用外部威胁情报数据资源，借助大数据分析技术，实现信息安全风险的量化管理。

- **看见未知风险：**从全新的外部视角识别多维度风险，例如：信息泄露、欺诈、劫持、僵尸网络、被封、异常流量等。
- **掌握威胁情报：**对全球 100+ 个威胁情报资源实时数据进行查询，每天进行风险识别和分析，掌握与企业相关的威胁情报。
- **量化风险分析：**用数据说话，量化安全风险，以数字表示安全状态，让安全风险更清晰可见、更容易管理。
- **第三方风险管理：**基于外部数据对合作伙伴、供应商进行安全评价，完成评估需求。保护业务和品牌的完整性。

Thank you!

了解更多

Web: www.aqzhi.com

Phone: 400-070-6887

Email: support@aqzhi.com

发邮件到这里获得邀请码，可以免费体验哦！