OWASP

Open Web Application Security Project

金融领域安全威胁分析及应对

李 洋

目录

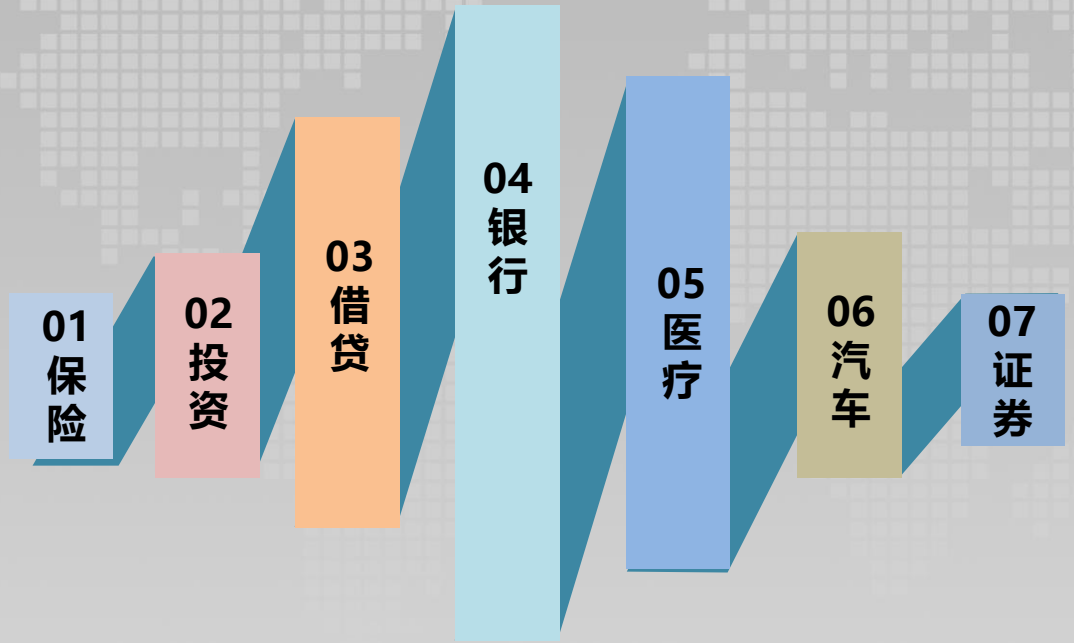
金融安全态势

互联网用户规模

国内互联网用户规模已超过7

亿！相当于欧洲人口总量！

涵盖众多领域



365易贷	团贷网	中国交通银行	现代财产保险	九州证券
91旺财	微贷网	中国民生银行	信诚人寿保险	南京证券
爱合投	温州贷	中国农业银行	信达保险	平安证券
爱钱进	信融财富	中国银行	幸福人寿保险	西部证券
爱投资	易通贷	中国邮政储蓄银行	新华保险	中航证券
贝格数据	宜信	中信银行	阳光保险	中山证券
贷贷兴隆	翼龙贷		亚太财险保险	中投证券
点名时间	银湖网	安邦保险	永安财产保险	中邮证券
分期乐	银票网	安华农业保险	永诚财产保险	
合时代	有利网	长安责任保险	友邦保险	
和信贷	云筹	长城人寿保险	中国大地保险	
慧择网	招商贷	长生人寿	中国平安保险	
互利网	众信金融	鼎和保险	中国人寿财产保险	
积木盒子	资本汇	都邦保险	中华联合财产保险	
金银猫		泛华保险	中融人寿保险	
九次方	北京银行	复星保德信	中银保险	
九斗鱼	朝阳银行	国元农业保险	紫金财产保险	
玖融网	广发银行	华安保险		
桔子分期	杭州银行	华农财产保险	渤海证券	
乐童音乐	恒丰银行	华泰财产保险	德邦证券	
陆金所	华润银行	华泰人寿保险	东方证券	
绿能宝	徽商银行	华夏人寿	东吴证券	
拍拍贷	江苏银行	江泰保险	方正证券	
钱爸爸	建设银行	利安人寿	广州证券	
乾贷网	南京银行	利宝保险	国都证券	
钱多多	宁波银行	民安财产保险	国联证券	

第三方支付　数字货币　……

平安的互联网金融

用户规模在百万以上的业务非常多，且持续在增长发展。

26

集团26家专业子公司

3.46亿

共有3.46亿的互联网用户

金融全牌照

业务覆盖支付交易、银行、证券、借贷、医疗、保险、资管、房产、汽车等领域

新领域探索

金融大数据、人工智能、区块链等

安全威胁

- 购物App
- 银行App
- 理财App
- 线下支付App
- 医疗保险App

- 大规模数据泄露
- 营销活动盗刷资损
- 风控体系不健全导致薅羊毛
- 安全漏洞泛滥
- 内网系统服务更新升级不及时
- 对新技术领域安全没感知

...

传统金融模式往互联网金融转型，安全未同步发展，仍停留在传统金融时的水平，攻防发展不对称

互联网金融安全事件频发，对业务将造成资金损失和极大负面影响。

01 ● 概览：金融安全态势

02 ● 分析：金融安全威胁

03 ● 应对：平安科技实践

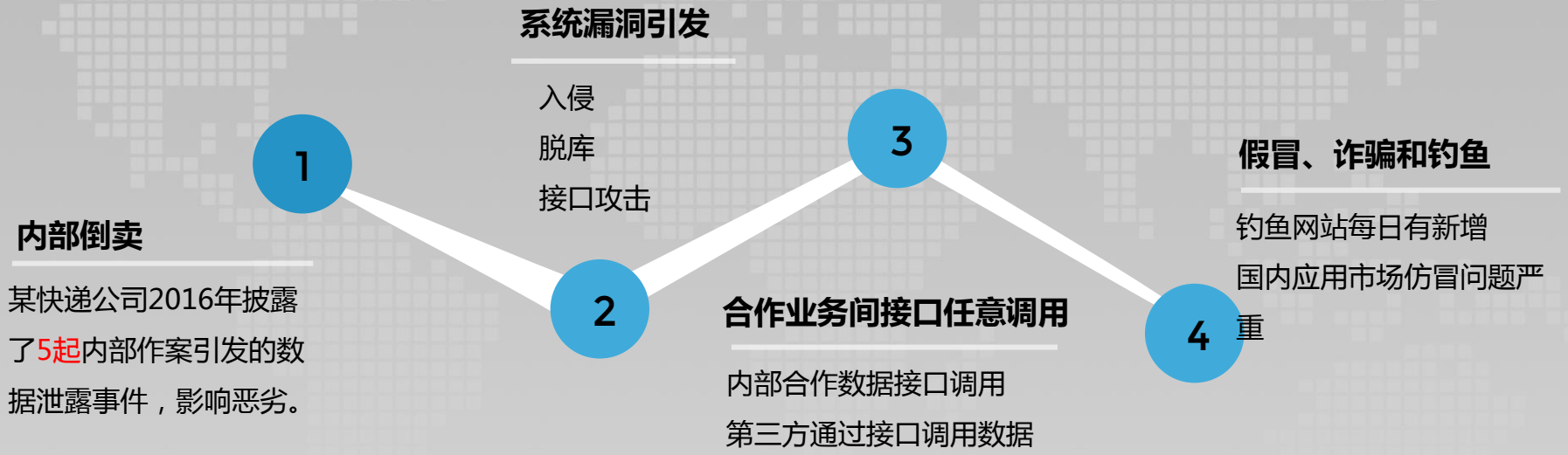
04 ● 推介：安全专家服务


TOP hreats
01
数据泄露防控
成为痛点
02
业务系统安全漏洞
普遍存在线上
03
风控体系不健全纵容
黑灰产薅羊毛猖獗、
资金盗刷屡见不鲜
04
攻击防护能力普遍不高
05
安全体系建设/安全保
障环节未落地
06
对金融新技术领
域安全没感知

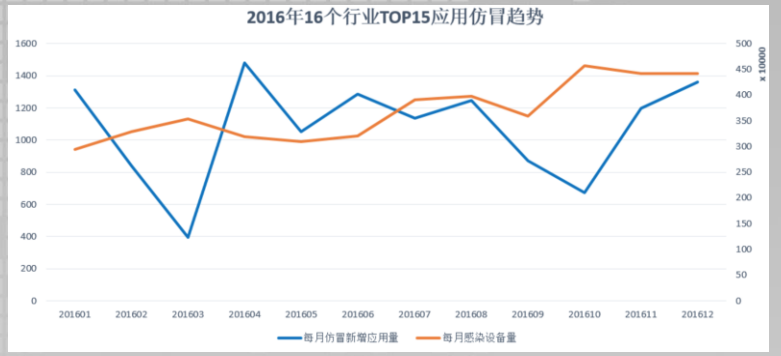
Threat TOP1—数据泄露

- 2016年全年全球发生数据泄露事件1200余起，被盗信息超过11.2亿条
- 2014年陆续发生的雅虎 5亿用户数据，及之后曝出的13年8月的10亿账户泄露事件，使得雅虎成为2016年数据泄露最大的“赢家”，甚至影响到其被收购价（下调3.5亿美元）
- 国内网民因数据泄露造成的损失更是达到 几百亿规模
- 大量数据泄露使得用户信息、业务数据被黑产灰产利用，导致了企业和用户更大的损失。

Threat TOP1——数据泄露



Threat TOP1——数据泄露



Rank	Financial threats	Impacted machines
1	Ramnit	460,673
2	Bebloh	310,086
3	Zbot	292,160
4	Snifula	121,624
5	Cridex	23,127
6	Dyre	4,675
7	Shylock	4,512
8	Pandemiya	3,330
9	Shifu	2,177
10	Spyeye	1,480

Threat TOP2—业务系统安全漏洞

权限控制问题最为严重

接口权限控制不当当值大量敏感信息泄露

普遍存在越权访问、操作问题

服务安全形势不容乐观

内网系统安全形势严峻

服务器漏洞组件升级不及时

PWN

互联网金融业务特有的逻辑漏洞

绑卡鉴权、转入转出

贷款、还款金额篡改

支付消费漏洞

其他常规类型漏洞

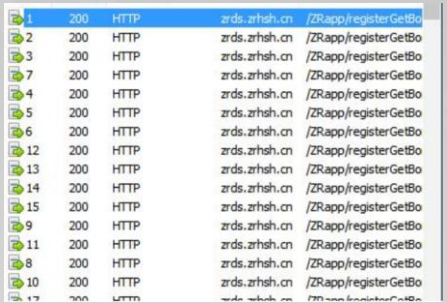
SQL注入

存储XSS

敏感信息未保护

Threat TOP3—风控体系缺失或不健全

- 国内黑产人员规模达160W，形成成熟运作产业链。
  个人信息已大量流入黑产人员手中，但受害者却一无所知
- 恶意注册、恶意绑卡、骗贷、盗刷、洗钱
- 人工薅羊毛
- 案例经验教训已经有很多，造成大量资金损失



Threat TOP4—攻击防护能力普遍不高

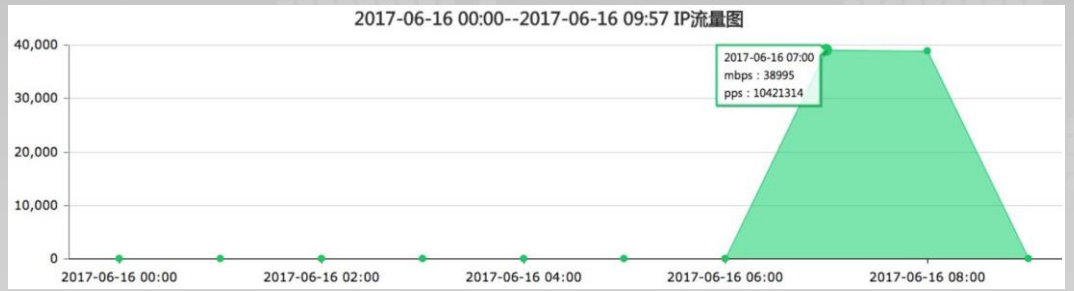
[redacted]:“无敌舰队”组织向国内多家证券金融公司发起DDoS比特币勒索

2017年06月16日

近期开始，国内多家证券、互联网金融公司接到DDoS威胁恐吓，境外黑客组织“无敌舰队（Armada Collective）”通过向国内企业发送邮件进行DDoS威胁，如果需要避免，需要向黑客组织支付比特币。

[redacted]云安全平台接到的最近的勒索事件发生在6月15日凌晨，黑客组织宣称将于6月21日将对[redacted]防护的某证券网站发起攻击。如果在攻击前向黑客组织支付10比特币（约合20万人民币），如果在攻击后再支付比特币，则勒索金额涨至20比特币，以后每晚一天，需要多支持10比特币。

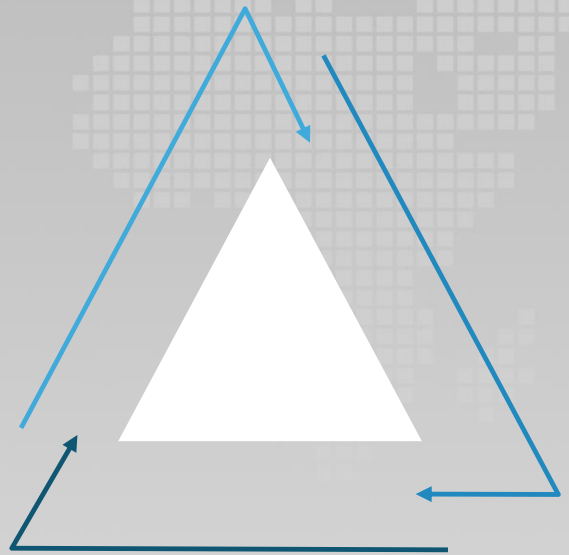
发件人: Armada Colle[redacted]ce.com>
收件人: [redacted]
日期: 2017/06/15 07:14
主题:Ransom request: DDoS Attack



Threat TOP5—安全体系建设未落地

安全体系化建设停留在纸面

未持续有效实施



应对监管或第三方

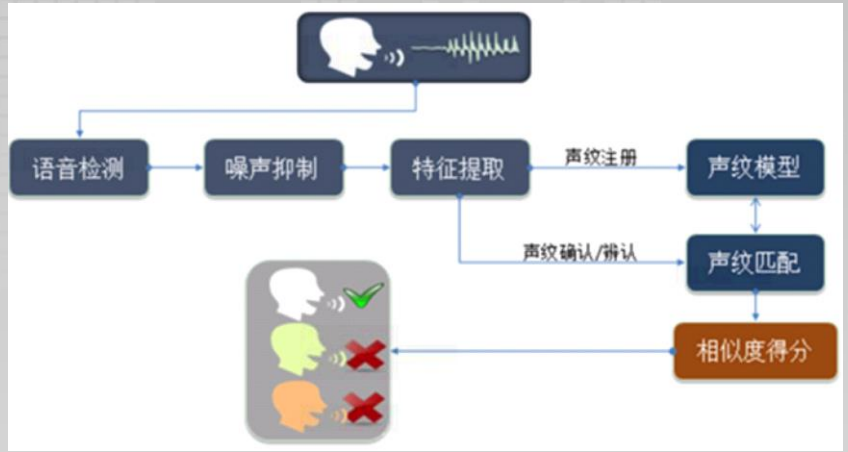
机构的安全检查

仅定期做安全测试，

很多新发布业务需求

未及时经过安全把关

Threat TOP6—金融新领域安全没感知



01 ● 概览：金融安全态势

02 ● 分析：金融安全威胁

03 ● 应对：平安科技实践

04 ● 推介：安全专家服务

立体化金融安全体系建设 & 落地

SDL安全运营	整个生命周期	专人跟进	闭环可控
安全咨询	一行三会监管规定	信息安全管理	等保认证
威胁情报响应	高危漏洞威胁	业务攻击威胁	7*24小时响应
安全解决方案	端到端服务	网络主机数据库设备	风险控制
风控体系	账号安全	设备指纹	防薅羊毛
威胁感知体系	高危漏洞检查	高危端口服务检查	Web漏洞检查
主机防护体系	服务器安全防控	入侵实时感知	攻击回溯
应用安全扫描	提高测试效率	三核检查引擎	定制化检查

金融安全SDL

安全培训

根据开发运营团队具体问题进行不定范围安全培训，提高安全意识和技能

安全测试

发版前进行人工和自动化测试，保障高、中漏洞不流入线上环境

应急响应

通过威胁情报系统主动收集业务相关安全风险，在第一时间进行闭环响应

安全评估

参与产品需求和安全设计，根据产品特性提出安全需求和设计方案。

安全运营

上线后对集成环境安全进行人工检测和自动化监控，确保安全风险在控制中。

其他安全实践

01 安全生态打造

02 定制化安全服务

03 金融安全研究

01 ● 概览：金融安全态势

02 ● 分析：金融安全威胁

03 ● 应对：平安科技实践

04 ● 推介：安全专家服务