因唯安全 所以信赖

唯与同行，智御未来

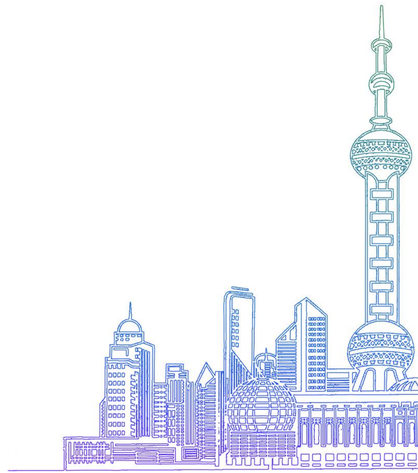
通用型漏洞的应急响应

主讲人：钟武强

腾讯安全应急响应中心（TSRC）负责人

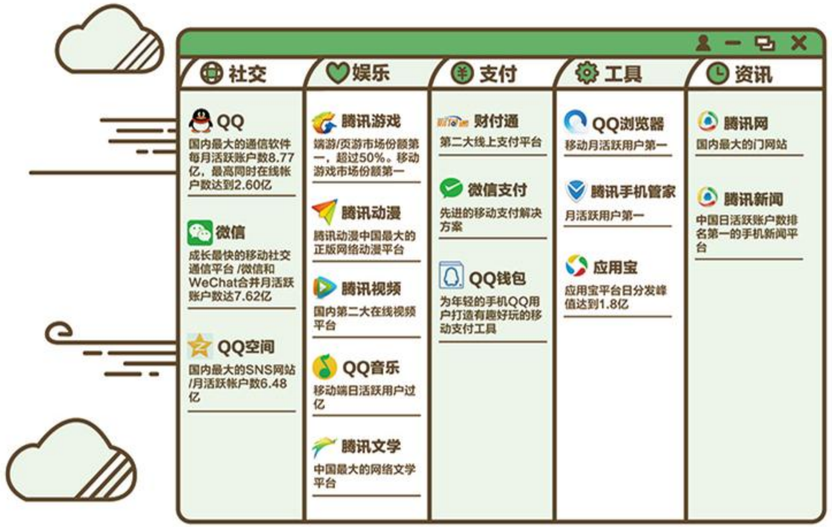
关于我

- 钟武强（小五），微信号Mark4z5
- 腾讯安全应急响应中心（TSRC）负责人
- 广东省信息安全测评中心 —> 百度 —> 腾讯
- 十多年安全经验，擅长应急响应、渗透测试



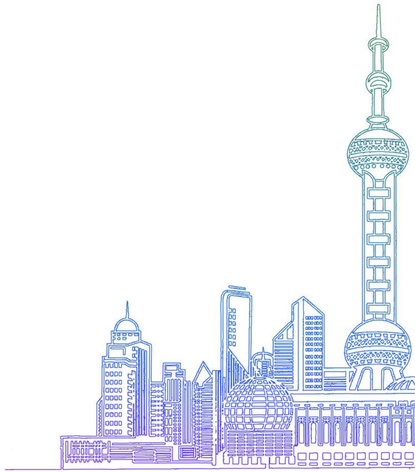
关于腾讯

- 中国最大互联网公司，全球市值排名第五
- 产品众多，形态多样化
- 超十亿用户，超百万台服务器



安全风险分类

业务安全	应用运维安全	内部安全
账号风险 欺诈风险 etc..	漏洞攻击风险 DDOS攻击风险 etc..	办公网攻击风险 员工违规风险 etc..



漏洞Case 1回顾

2014年 OpenSSL Heartbleed心脏出血漏洞

远程读取服务器内存数据

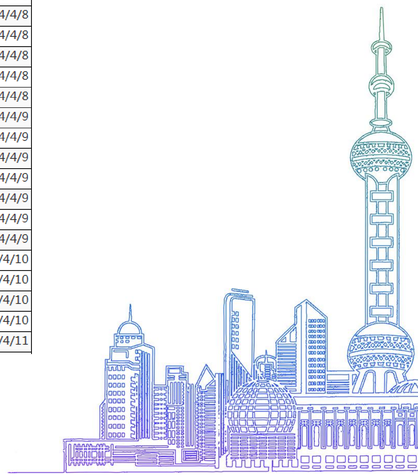
发送https恶意请求就能窃取到其他用户cookie凭证

各大互联网公司受影响

修复方案：升级OpenSSL并重启WebServer等服务

国内某漏洞平台收到的报告

漏洞标题	提交日期
[redacted]“心脏出血”漏洞可读取敏感信息	2014/4/8
[redacted]主站运维不当导致可以登录随机用户并且获取服务器敏感信息	2014/4/8
[redacted]中国运维不当导致随机用户明文密码泄漏	2014/4/8
[redacted]“心脏出血”泄露用户信息	2014/4/8
[redacted]运维不当可导致泄漏敏感信息	2014/4/8
[redacted]运维不当导致泄漏敏感信息	2014/4/8
[redacted]运维不当导致可能存在随机登录银联账户并获取服务器敏感信息	2014/4/8
[redacted]运维不当导致敏感信息泄漏	2014/4/8
[redacted]通行证服务器运维不当导致信息泄露	2014/4/8
[redacted]主站运维不当导致可以登录随机用户并且获取服务器敏感信息	2014/4/8
[redacted]运维不当导致可能存在随机登录账户并获取服务器敏感信息	2014/4/8
[redacted]运维不当员工邮件内容泄露	2014/4/9
任何平台任何使用openssl库的程序都可能受到攻击（非https）	2014/4/9
[redacted]邮件服务器openssl漏洞导致敏感信息泄露	2014/4/9
[redacted]营运维不当导致敏感信息泄漏	2014/4/9
[redacted]网盘运维不当导致敏感信息泄漏	2014/4/9
[redacted]大学VPN运维不当导致敏感信息泄漏	2014/4/9
[redacted]运维不当导致敏感信息泄漏	2014/4/9
[redacted]网运维不当导致可能存在随机登录账户并获取服务器敏感信息	2014/4/10
[redacted]运维不当导致可获取服务器敏感信息	2014/4/10
[redacted]网站运维不当导致敏感信息泄漏	2014/4/10
[redacted]大学某站配置不当	2014/4/10
[redacted]某版本OPENSSL heartbleed 通杀	2014/4/11



漏洞Case 2回顾

2016年 ImageMagick远程代码执行漏洞

上传一张图片就能入侵服务器

各大互联网公司受影响

国内某漏洞平台收到的报告

漏洞标题	提交日期
某漏洞导致直接Getshell影响主干网络直入内网	2016/5/5
存储远程命令执行漏洞影响图片处理服务器	2016/5/5
某处命令执行	2016/5/5
某处命令执行	2016/5/5
主站某处命令执行自带NMAP(影响内网数百主机安全)	2016/5/5
存在远程命令执行漏洞	2016/5/5
某站远程命令执行	2016/5/5
主站命令执行	2016/5/6
某子站点远程执行命令	2016/5/6
主站ImageMagick命令执行三处	2016/5/6
某站存在命令执行	2016/5/6
某站命令执行漏洞	2016/5/6
主站远程命令执行	2016/5/6
图片服务器命令执行(已入内网)	2016/5/6
官方APP远程命令执行	2016/5/6
直播APP命令执行	2016/5/7
主站命令执行已反弹shell入内网	2016/5/7
某服务器的两处命令执行可shell	2016/5/8
车官方app命令执行	2016/5/8

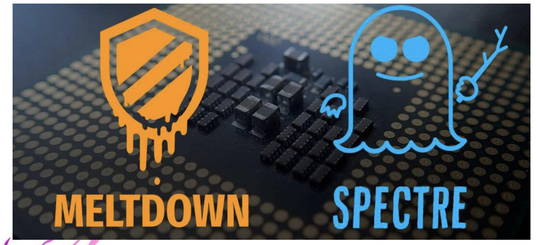
国外某互联网巨头公司被爆漏洞

IMAGETRAGICK STORY

Timeline:

16 Oct 2016, 03:31 am: Initial report
18 Oct 2016, 05:35 pm: Actual PoC I used requested by security team member Neal
18 Oct 2016, 08:40 pm: I replied by sending a PoC and provided additional info
18 Oct 2016, 10:31 pm: Bug acknowledged by security team member Neal
19 Oct 2016, 12:26 am: Just heads-up by security team member Neal that fix is in the progress
19 Oct 2016, 02:28 am: Neal informed me that vulnerability has been patched
19 Oct 2016, 07:49 am: I replied confirming that the bug was patched and requested disclosure timeline
22 Oct 2016, 03:34 am: Neal answered about disclosure timeline
28 Oct 2016, 03:04 pm: $40k reward issued
04 Nov 2016: Reward paid through Bugcrowd payment system
16 Dec 2016: Disclosure approved

漏洞Case 3回顾



2018年 Intel CPU信息泄漏漏洞

几乎全部Intel CPU受影响

修复方案：打微码补丁、操作系统补丁

重启系统、性能下降，还可能蓝屏

Windows补丁修出1个本地提权漏洞 Orz

Intel CPU架构漏洞越捅越大 打补丁将损失30%性能_凤凰科技

2018年1月3日 - 光看这种行动的规模就知道这次爆出的漏洞有多严重了。 本次爆出的Intel CPU架构漏洞的具体表现为核心内存泄漏,是属于芯片级别的安全bug,这个bug迫使Li...

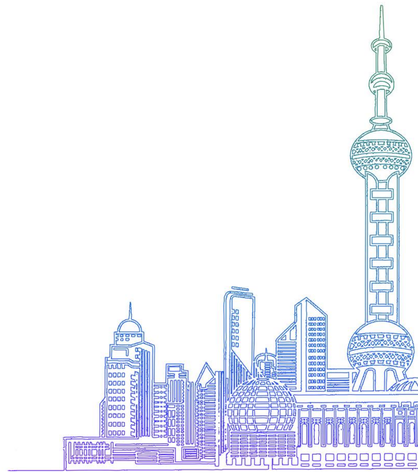
tech.ifeng.com/a/20180... - 百度快照

[图]Windows 7装CPU漏洞补丁后出现蓝屏 安全模式也进不了 - ...

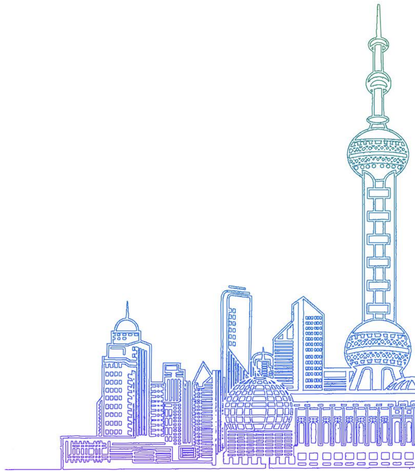
2018年1月8日 - 导致不兼容AMD Athlon 64 x2处理器问题之后,近日又有消息称微软面向Windows 7系统发布的KB4056894存在升级失败问题,导致错误代号为0x000000c4的蓝屏情...

https://www.cnbeta.com/article... - 百度快照

所以 通用型漏洞 往往影响范围广，修复难度大，处理非常棘手



腾讯是如何开展通用型漏洞的应急响应？



应急响应流程

第一阶段

漏洞获悉
漏洞评估

第二阶段

漏洞知会
漏洞发现
漏洞修复
攻击检测
攻击拦截

第三阶段

复盘总结
价值输出

漏洞获悉
漏洞评估

没弄到情报？

情报来晚了，被搞了？

好多情报，看不过来？

- 情报自动化采集
  - 200个软件源、100个资讯类源、400个twitter微博源
  - 平均每15分钟采集一轮，日均采集1000条
  - 过滤后日均推送告警80条，紧急情报重点提醒
- 漏洞奖励计划
  - 0day 或 最新公开漏洞情报
- 自主挖掘发现
- 其他渠道
  - 官方保密性漏洞通知（如Intel）
  - 私人圈子交流

漏洞获悉
漏洞评估

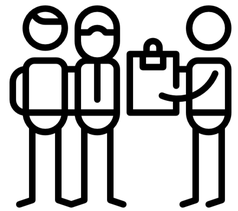
评估速度慢？

评估误判？

- 评估要点
  - 确认漏洞原因、危害、影响范围、PoC和修复方案
- 评估效率及准确性
  - 关键是人才，安全技术及经验的积累

漏洞知会
漏洞发现
漏洞修复
攻击检测
攻击拦截

- TSRC作为应急指挥中心，统一协调确保各项应急工作有序、快速开展
- 第一时间通知安全兄弟团队、公司领导、业务同事，告知风险及后续工作



漏洞知会
漏洞发现
漏洞修复
攻击检测
攻击拦截

如何全面发现
存在漏洞的业务？

- 主机安全系统本地采集受影响主机
  - 本地执行find/ps/grep/strings/ldd/特定二进制等命令
- 漏洞扫描器对全业务Web/APP进行检测
- 人工排查重点业务，优先保证重点业务安全
- 引导业务同事进行自查
- 白帽子帮忙发现漏网之鱼

漏洞知会
漏洞发现
漏洞修复
攻击检测
攻击拦截

修复优先级？

修复闭环？

漏洞咨询量暴增？

- 邮件/微信/工单等方式通知业务修复
  - 给出修复方案和限期，外网优先修复
  - 使用工单系统进行闭环，避免跟丢
  - 持续确认和周知修复情况
- 漏洞FAQ文章，减少沟通成本

漏洞知会
漏洞发现
漏洞修复
攻击检测
攻击拦截

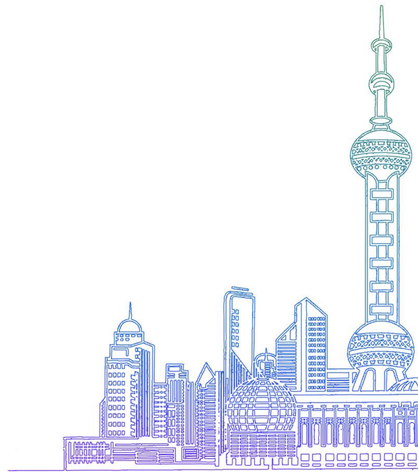
修复期间遭攻击？

- 网络入侵检测系统（4/7层异常流量）
- 主机入侵检测系统（webshell、命令执行等）

漏洞知会
漏洞发现
漏洞修复
攻击检测
攻击拦截

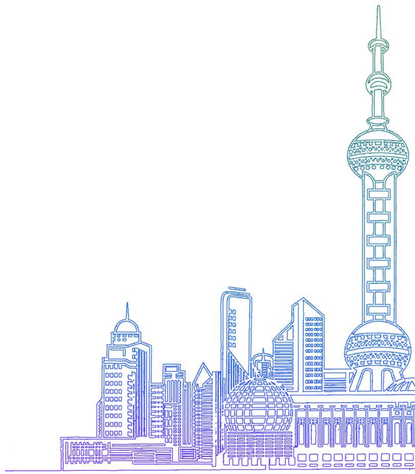
修复期间遭攻击？

- Web应用防火墙（WAF）拦截恶意请求
- 主机入侵检测系统具备快速止损能力
  - 一检测到攻击成功，立刻断网



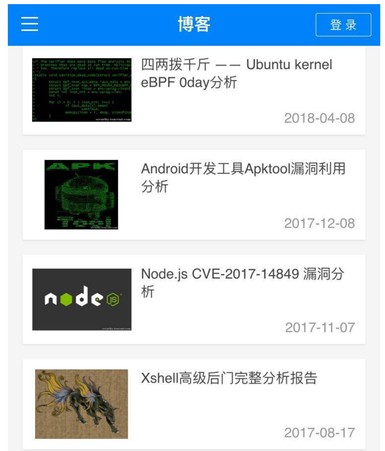
复盘总结
价值输出

- 按时间线整理应急过程，肯定成绩，暴露缺陷
- 举一反三，提升安全能力，避免长期疲于救火



复盘总结
价值输出

- 发表内部文章，宣传安全价值，赢取业务持续配合安全工作
- 发表外部文章，分享安全技术，为互联网安全贡献力量



腾讯TEG安全平台部

- 漏洞扫描
- 入侵检测
- 态势感知
- WAF拦截
- DDOS防御
- 业务安全
- 安全大数据

- 应急响应
- 红蓝对抗
- 安全评估
- 安全预研
- AI安全
- etc..

负责全公司安全问题，每天枪林弹雨，挑战巨大

有挑战才有进步，欢迎加入我们

https://security.tencent.com

security@tencent.com

谢 谢 观 看 ！

2018 唯品会第三届互联网电商安全峰会

2018 vip.com third Internet ecommerce Security Summit

2018-5-5 上海