【倒计时10day】看雪论坛精华优秀文章分享与点评

转载

weixin_33674976 于 2018-12-22 17:58:00 发布 50 收藏

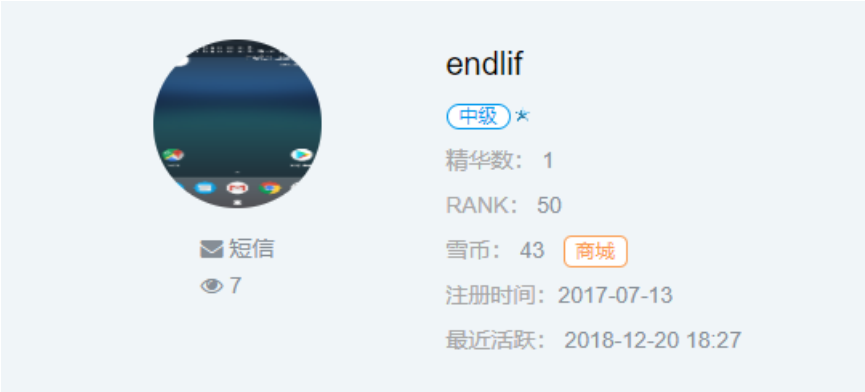
不知不觉，我们就到了2018倒数第二个周六啦，最后关头又有哪些好文章诞生呢，我们一起来看一下~

1

『Android安全』

1、 从补丁到Root——CVE-2014-4323分析

作者：endlif

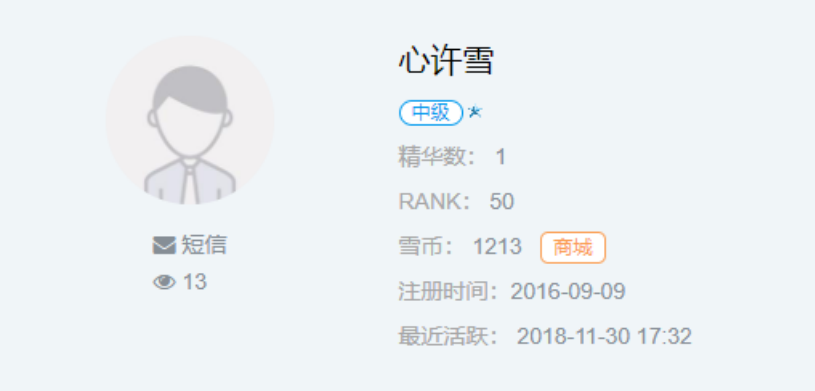


上榜：**精华**

点评：这篇漏洞分析是从漏洞补丁开始反推漏洞利用，并列出了三种提权的思路。此文还让读者了解了内核崩溃的三种类型，和查看崩溃日志的方法。

2、(Android Root)CVE-2017-7533 漏洞分析和复现

作者：心许雪

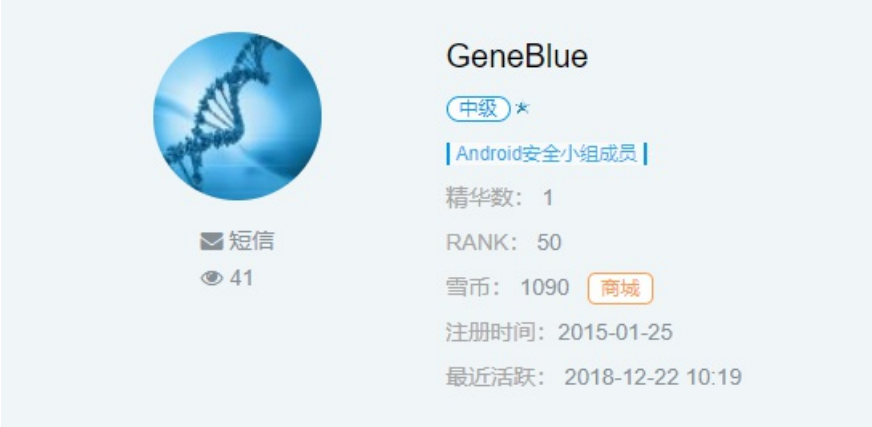


上榜：**精华**

点评：本文记录了CVE-2017-7533的漏洞类型、漏洞原理、如何触发，如何被patch，并进一步在pixel2上复现了该漏洞。最后，还思考了从poc到exploit需要做哪些事情。

3、 KSMA-- Android 通用 Root 技术

作者：GeneBlue

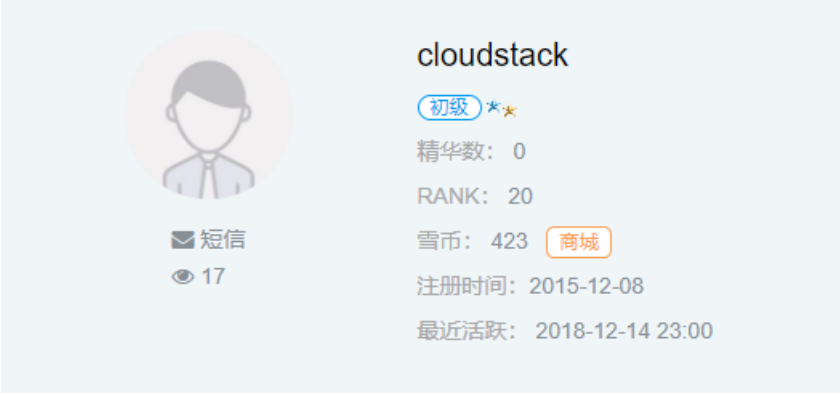


上榜：**精华**

点评：本文介绍了阿里巴巴的安全研究员ThomasKing发明的通用root方式KSMA（Kernel Space Mirroring Attack，意为内核空间镜像攻击），并深入研究了linux页表的原理。

4、记一次Android后门分析实战

作者：cloudstack



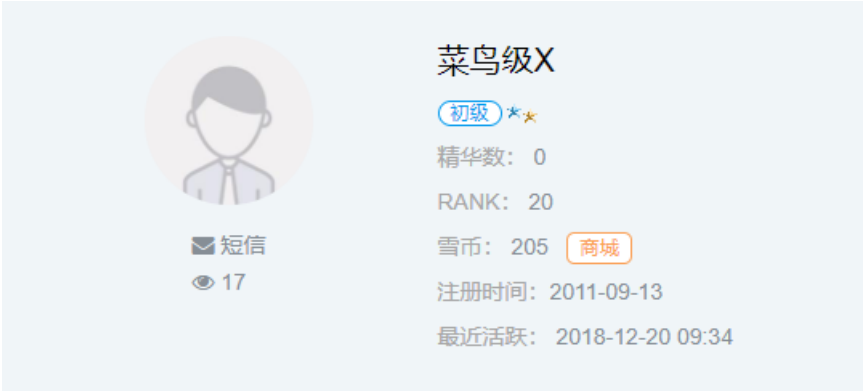
上榜：**优秀**

点评：本文从一个偶然发现的system进程出发，分析了ChiMaster.apk、chimahelper.apk两个恶意的apk样本文件，详细研究了关键函数的实现过程。

『编程技术』

1、【编译原理】FIRST集、FOLLOW集算法原理和实现

作者：菜鸟级X

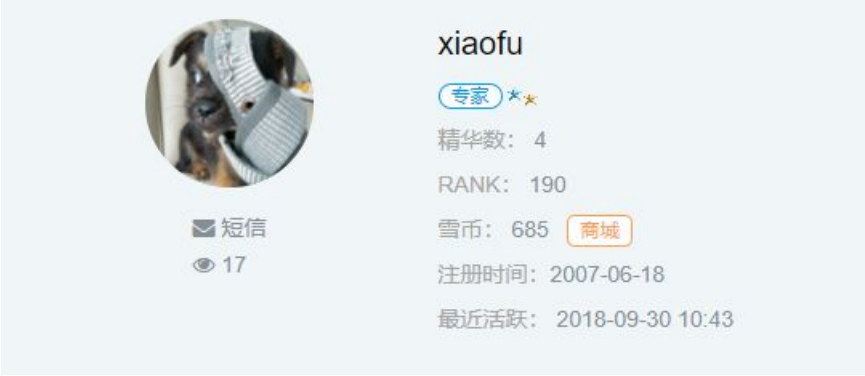


上榜：**优秀**

点评：菜鸟级X本文解读了著名的《编译原理》书中FIRST集、FOLLOW集算法原理的重点部分，并根据对算法的理解提供了代码实现。

2、 GxxeRpcs中的内存hash算法

作者：xiaofu



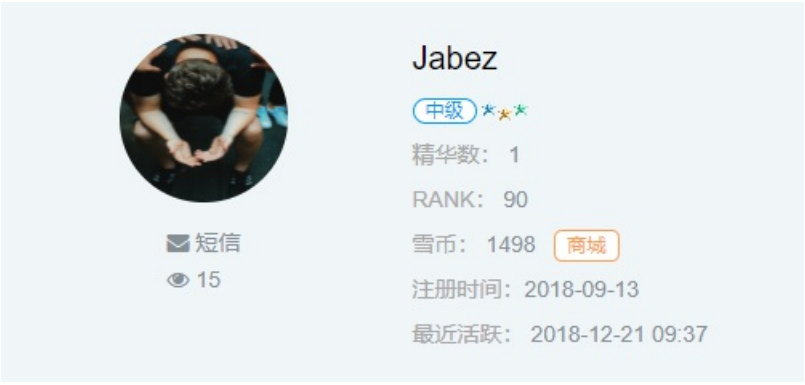
上榜：**优秀**

3

『加壳脱壳』

1、 脱壳之未知加密壳

作者：Jabez



上榜：**精华**

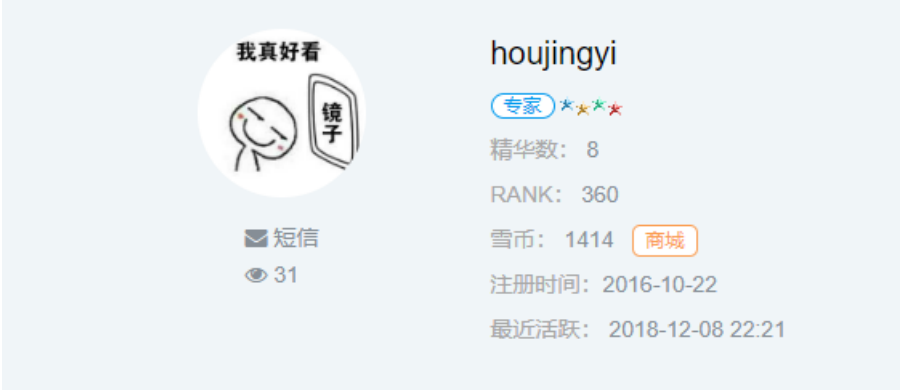
点评：本文较为详细地记录了脱去一个未知加密壳的步骤。文中分析了壳当中生成加密IAT的步骤，并通过图文展示了一系列的技术实践方法。

4

『二进制漏洞』

1、关于CVE-2017-8890的一点细节

作者：houjingyi



上榜：**精华**

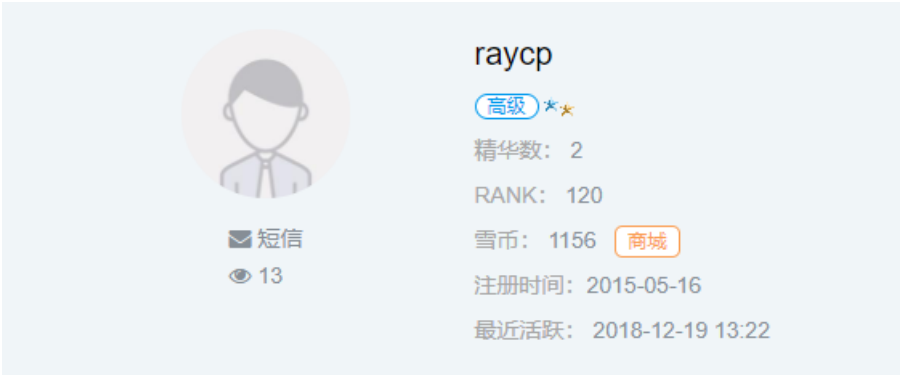
点评：本文主要总结了CVE-2017-8890漏洞中要注意的细节，起到了抛砖引玉的效果，最后给出了漏洞利用的代码。

5

『Pwn』

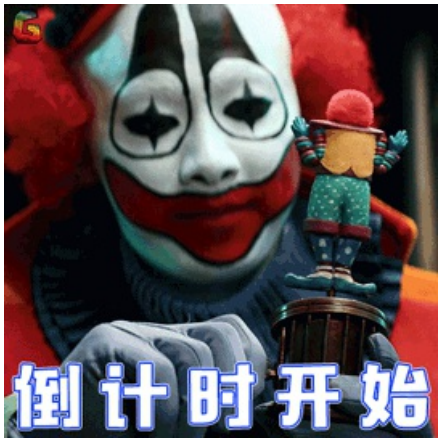
1、hctf 2018 部分pwnwriteup

作者：raycp



上榜：**精华**

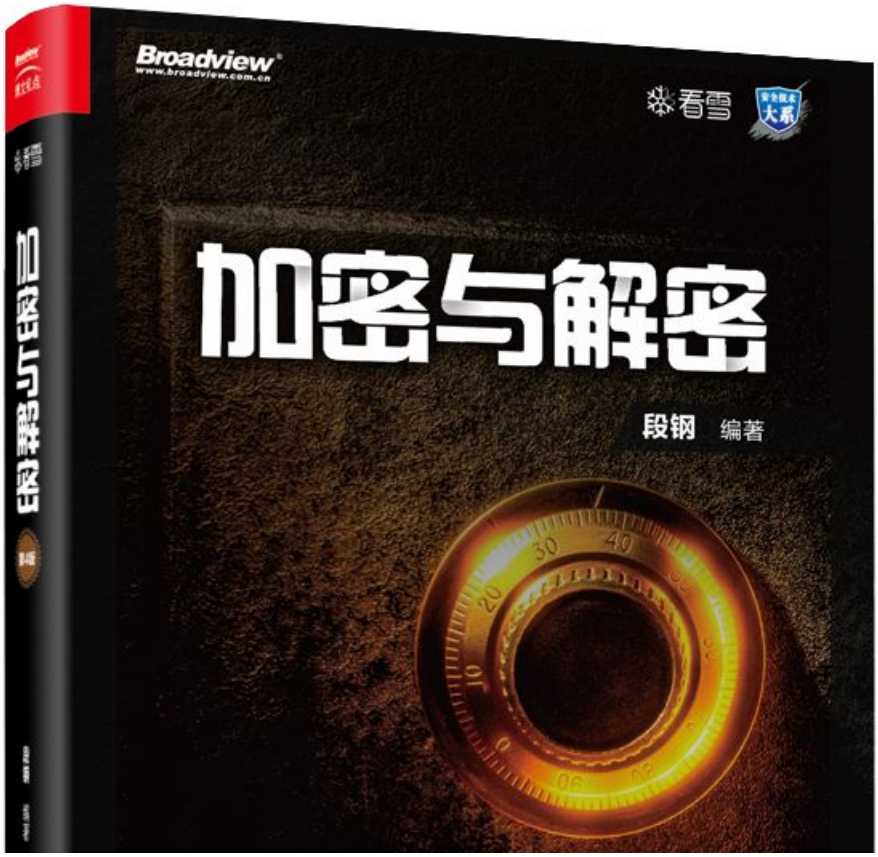
最后十天倒计时开始啦~！

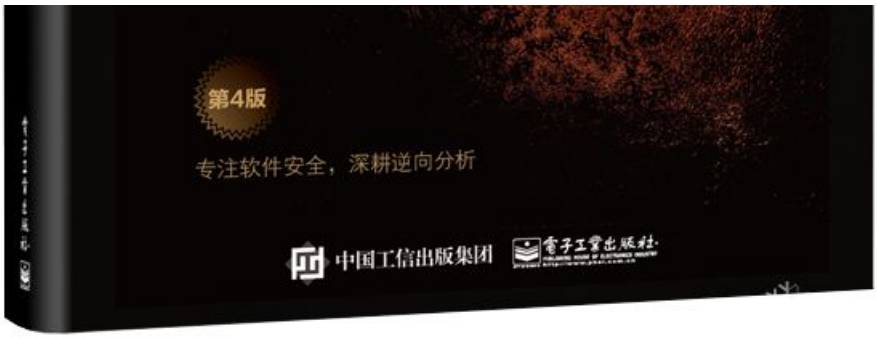


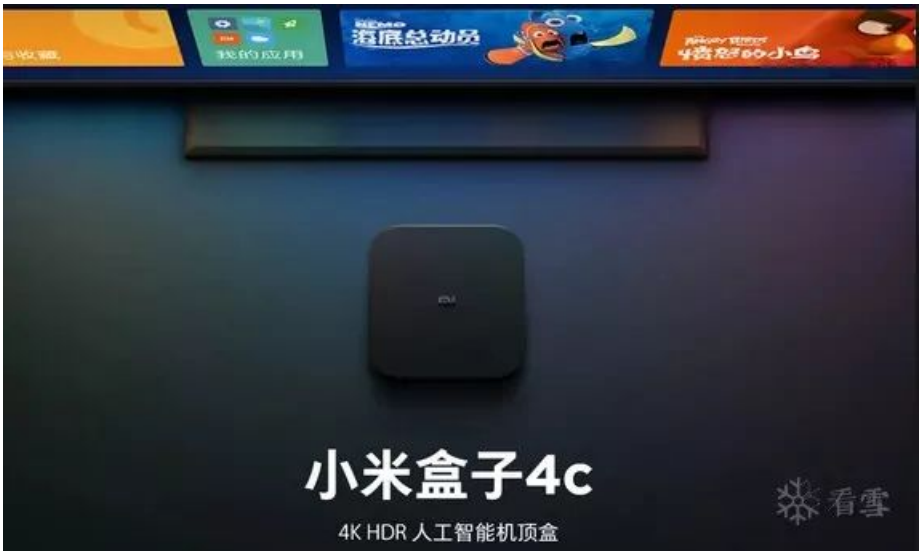
2018结束之际，我们将会评选出年度最佳原创技术文章，想要赢得丰厚奖品吗？快来看雪论坛留下你的原创文章吧~

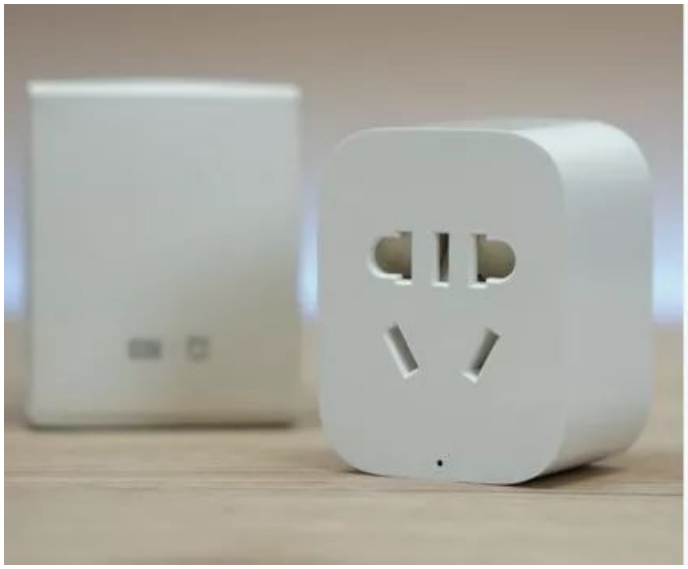
签名第4版《加密与解密》+小米AI音响+小米盒子+米家（MIJIA）小米智能插座+1000雪币

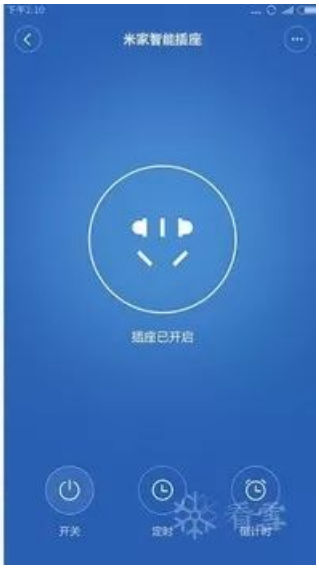
正在仓库等你带它走！




第4版
专注软件安全，深耕逆向分析
中国工信出版集团


我的应用
海底总动员
小米盒子4c
4K HDR 人工智能机顶盒




米家智能插座
插座已开启
开关
定时
倒计时

点击阅读原文，了解评参赛评选~！

还在等什么，快来投稿吧！

- End -

公众号ID：ikanxue

官方微博：看雪安全

商务合作：wsc@kanxue.com