人手一份核武器 - Hacking Team 泄露（开源）资料导览手册

转载

weixin_34059951 于 2018-03-08 10:57:53 发布 113 收藏
文章标签： 操作系统 移动开发 git
原文链接：https://juejin.im/post/5aa11731f265da23870e68e3

> 蒸米 · 2015/07/08 9:59

0x00 序

事先声明本人并不是全栈安全工程师，仅仅是移动安全小菜一枚，所以对泄漏资料的分析难免会有疏忽或着错误，望各位围观的大侠手下留情。

首先来看安全界元老对Hacking Team(以下简称HT)被黑这个事件的看法：

@tombkeeper: Stuxnet 让公众知道：“原来真有这种事”，Snowden 让公众知道：“原来这种事这么多”，Hacking Team 让公众知道：“原来这种事都正经当买卖干了”。

@赵武在路上: 2011年的时候，HBGray被黑，很多人没有意识到意味着什么，因为跟国家安全相关。这两天Hacking team被黑，大家也没有意识到意味着什么。这次包括了客户清单和0day，但我更关注的是RCS的代码，以前行业内都是粗糙到不行的demo，工程化公开的很少，这次会让行业内的技术往前推进几年，尤其是黑产。

可以说这次事件和斯诺登事件的影响力是不相上下的，但HT被黑不光光是让公众知道有这回事，随之而来还有整整415G的泄漏资料！里面有Flash 0day, Windows字体0day, iOS enterprise backdoor app, Android selinux exploit, WP8 trojan等等核武级的漏洞和工具。那么废话不多说，我们这就开始导览之旅。

0x01 总览

因为所有文件加起来的大小整整有415.77G。光下载就得好久好久。还好有人把整个镜像放了一份在网上。有兴趣的同学可以直接去查看：http://ht.transparencytoolkit.org/。据说之所以这么大是因为里面有很多的邮件。但你不用担心你的小水管，有好人整理了一个只有1.3G的精华版。在这里我也提供一个百度网盘下载：http://pan.baidu.com/s/1i3lHQRF 。在下载完完整版之前，我们就先拿精华版解解馋吧。

里面的数据大概是这样的：

“HACKING TEAM PASSWORDS AND TWEETS.pdf” 里主要保存了Christian Pozzi这个人经常去的网站的账号以及密码以及twitter的截图。估计他就是那个被黑了电脑的人了，因为这个人的电脑被黑，连带着HT内网git服务器，知识库，邮件服务器的数据全部都被dump下来了。

Hacking Team Saudi Arabia Training.pdf里面数据貌似不全，通过提纲来开看主要是介绍了如何安装和使用RCS (Remote Control System)系统。不得不说HT最牛的东西就是他们的RCS系统了，他们公司实现了全平台的RCS系统（包括windows phone）。我们可以看一下他们系统的截图：

各种监控信息详细到令人发指。不知道有多少人被这样监控着。

gitosis-admin-master.zip里保存了git服务器上成员的public key以及每个人负责的项目，通过”gitosis.conf”就可以大概知道哪个项目是谁在做了。比如placidi这个成员主要做android相关的项目。Naga, daniele, zeno, diego, ivan这几个人组要做fuzzer。Matteo, zeno, daniele这几个主要做病毒查杀检测。

所以接下来的章节我们也会按照他们的分组来进行分别讲解。

0x02 Android

---

1 core-android-audiocapture-master.zip主要是利用Collin Mulliner提供的hook框架来hook mediaserver从而进行语音和通话监听。”Pack”文件夹里保存了最后编译完成的程序。而”references”文件夹里几乎都是Collin Mulliner论文的ppt，并且整个项目就是在 https://github.com/crmulliner/adbi这个项目上改的。截取下来的音频并不是 wav格式，还需要使用”decoder”文件夹下的工具进行解密，看样子作者除了电话监听，还成功测试了wechat, whatsapp, skype等应用的语音截获。

2 core-android-market-master.zip应该是用来向Google Play上传监控应用的项目。虽然说Google Play检测系统，但对于这种用于APT攻击的malware是毫无作用的。在\core-android-market-master\doc\readme.txt中还保存HT开发者账号的用户名和密码。但是当笔者准备尝试登录的时候，发现密码已经在几个小时前被修改了。

3 core-android-master.zip就是HT的RCS系统源码了。除去一些编译用的gradle文件，所有的源码都保存在” \core-android-master\RCSAndroid”目录下，通过这个RCS app除了可以做到基本信息监控外，还可以获取所有主流社交应用的信息。

在应用加固方面，这个RCS app除了使用了DexGuard进行混淆，还有虚拟机检测功能。根据开发日志，这个项目貌似还使用很多0day的trick对应用进行混淆。非常值得以后慢慢研究。 接下来就是重头戏root了，主要代码都在\core-android-master\RCSAndroid\jni 这个目录下， 上来就能看到” exploit_list.c”这个霸气的文件，里面可以调用各种exp来获取root权限：

除此之外，core-android-master\RCSAndroid\jni\selinux_exploit还有绕过 selinux enforcing模式的exploit。

4 core-android-native-master.zip中有更加详细的root项目代码和说明，在”legacy_native”文件夹中：Suidext中包含了所有的shell。Local2root中包含了<=4.1版本的root exp。在”selinux_native”文件夹中，”Put_user_exploit”: 包含了 put_user calls的exp。”Kernel_waiter_exploit”包含了towelroot的exp。Suidext包含了新的shell。使用” build.sh”编译完后的exp都在”bin”目录下（这些exp是可以干掉android 5.0 selinux的）。其他的文件请参考目录下的README.txt。因为是意大利语，请使用Google自行翻译一下。

0x03 iOS & Mac OS

---

1 “core-ios-master.zip”里面的” core”文件夹中保存了RCS的主要代码。主要是利用dylib注入对用户输入，GPS，屏幕等信息进行监控。

”ios-newsstand-app”文件夹应该是另一个ios应用的源码。看代码大概是替换ios系统的输入法，然后进行键盘记录，大概是用来攻击没有越狱的机器吧。”Keybreak”文件夹是用来破解手机锁屏密码的，里面有lockdownd remote exploit的源码。”ios-install-win32”和” ios-install-osx”文件夹里是windows和mac os下来给iPhone或者iPad装应用的工具。此外HT还拥有一个iOS enterprise帐号可以用来发布enpublic app: “UID=DE9J4B8GTF, CN=iPhone Distribution: HT srl, OU=DE9J4B8GTF, O=HT srl, C=IT”。关于enpublic app的危害，可以参考我之前的文章或论文。

2 “vector-ipa-master.zip”里面应该是另一个ios木马的源码，这个木马并不是应用，貌似是一个底层网络代理，可以用来监控或者控制系统的网络流量。

3 “core-macos-master.zip”的”core-macos-master\core”的文件夹中保存了mac os RCS的源码，其实就是mac os木马了，和windows的木马非常相似。

0x04 Windows Phone & symbian & blackberry

1 `core-winphone-master.zip`是Windows Phone的RCS木马。据说在WP设备上实现“激活追踪”是利用了系统中的一个0day，允许第三方代码程序像受信任程序一样执行。该RCS还可以获取联系人、日历、通话、地理位置、短信、传感器状态状态等信息。程序ID为：`11B69356-6C6D-475D-8655-D29B240D96C8`。

2 `core-blackberry-master.zip`和`core-symbian-master.zip`分别是黑莓和塞班的RCS系统。

0x05 Fuzzer

`fuzzer-windows-master.zip`主要保存了windows下的fuzzer源码。里面有针对IE和字体的Fuzzer测试系统。

`fuzzer-android-master.zip`主要保存了android下的fuzzer源码。里面有针对jpg，sms和system call的Fuzzer测试系统。Trinity主要是用来做system call fuzzer的，比如说binder使用的ioctl()系统调用。

0x06病毒查杀检测

`test-av-master.zip`是第一代产品。`test-av2-master.zip`是第二代产品。HT给他们起名叫AVMonitor。这个系统主要使用来做查杀检测，用来保证自己的产品可以通过检测。`test-av2-master.zip\test-av2-master\doc\AVTEST Box.xlsx`保存了他们使用的杀毒软件的列表和序列号。

在”test-av2-master\doc\whiteboard”文件夹中甚至有他们开会的白板照。

0x07 Exploit & 0day

`vector-exploit-master.zip`文件又是第二波高潮的开始，首先在里面你可以找到两个flash的exp: 一个是Flash的0day : `ActionScript ByteArray Buffer Use After Free`，另一个是Nicolas Joly在Pwn2Own 2015大赛中使用的CVE-2015-0349。为了在IE和Chrome上绕过其沙盒机制完全控制用户系统，Hacking Team还利用了一个Windows中的内核驱动： Adobe Font Driver(atmfd.dll)中存在的一处字体0day漏洞，实现权限提升并绕过沙盒机制。该0day漏洞可以用于WindowsXP~Windows 8.1系统，X86和X64平台都受影响。数字公司已经在很多人种子还没下完的时候就写出了分析报告：http://drops.wooyun.org/papers/6968，有兴趣的读者可以前去围观。

除了flash的两个exp和font 0day外，在`vector-exploit-master\src\ht-webkit-Android4-src`目录下还有一个Android Browser exploit，在用android brower浏览一个网页后就可以在目标机器上安装上目标apk。该漏洞会影响Android 4.0.*到4.3.*版本的手机。粗略看了一下源码，利用过程十分复杂，exp的利用至少有四个stage，还用到了information leak，heap spray等技术。PS:在`vector-exploit-master\src\ht-webkit-Android4-src\docs`中有公司开会的时候拍的exp图解。

0x08 其他

1. `GeoTrust-master Signing Keys.zip` 保存了HT的GeoTrust证书。
2. `http://ht.transparencytoolkit.org/audio/` 里有大量的录音。

3. HT在自己家的产品中留下了SQL后门，方便他们随时查询。http://ht.transparencytoolkit.org/rcs-dev%5cshare/HOME/ALoR/htdocs/conf.php

   虚拟机保护壳VMProtect Professional的很多正版key泄漏

   https://ht.transparencytoolkit.org/rcs-dev%5cshare/HOME/ALoR/VMProtect.key
   https://ht.transparencytoolkit.org/rcs-dev%5cshare/HOME/Ivan/vmprotect/

0x09 八卦

---

1 Phineas Fisher号称自己黑了gamma和HT。HT的twitter还转发了这条消息。。。

2 HT的密码都特别简单，不被黑才怪。

3 http://ht.transparencytoolkit.org/c.pozzi/Desktop/you.txt 你懂的。。。(from @youstar)

0x0a 未完待续

由于泄漏的资料实在太过庞大，本文还有很多的内容没有覆盖到。因此我们在随后的几天还会继续跟进这个事件，并更新我们的文章，欢迎大家回来继续阅读。

0x0b 更新2015.7.10

---

1 HT泄漏中大家最关心的就是Flash 0day了，通过这个0day黑客可以让用户在浏览一个网页后就被黑客远程控制。这里我们给出一个POC（概念验证）网页供大家测试：http://zhengmin1989.com/HT/index.htm 该网页并不会安装恶意程序到你的电脑，但是会执行calc.exe命令唤起计算器程序。当然黑客也可以把计算器程序换成别的恶意程序或者直接执行del .等恶意指令，所以如果你弹出计算器了话赶紧去安装补丁吧！另外不要以为自己用的非主流的浏览器就不会中招，这些非主流的浏览器内核都是直接用主流浏览器的开源框架，只是换了个壳罢了。比如说这个115浏览器，该弹的一样会弹啊。

2 另外Windows中的内核驱动Adobe Font Driver(atmfd.dll)中存在的字体0day漏洞也有demo。可以在http://zhengmin1989.com/HT/32bitwin81.zip下载，本人已经在win8上测试成功了。

3 为了方便大家分析HT的项目源码，有人将HT的git服务器上传到了github并且对每个项目进行了一些简单说明，并且还在持续更新：https://github.com/hackedteam?tab=repositories 但说明都是英文版的，如果想要看中文版可以参考绿盟科技在drops发表的《简要分析Hacking Team 远程控制系统》：http://drops.wooyun.org/papers/7025

4 之前提过泄漏资料中绝大多数内容是邮件，Wikileaks已经把泄漏的所有邮件都放在他们的在线数据库中了，可以非常方便的进行搜索。地址是：https://wikileaks.org/hackingteam/emails/ 里面可以搜到很多劲爆邮件，比如HT在NSA的后门等。

5 在泄露的资料中可以找到HT的客户名单，甚至包括美国的FBI，一共有41,871,712 欧元生意：https://ht.transparencytoolkit.org/Amministrazione/01%20-%20CLIENTI/5%20-%20Analisi%20Fatturato/2015/02%20-%20Client%20Overview%202015/Client%20Overview_list_20150603.xlsx