

HGAME 2022 Week1 writeup by Halo

HGAME 2022 Week1 writeup by Halo

CRYPTO

RSA Attack 3

IoT

饭卡的UNO2.0

MISC

卡中毒

WEB

Vidar shop demo

CRYPTO

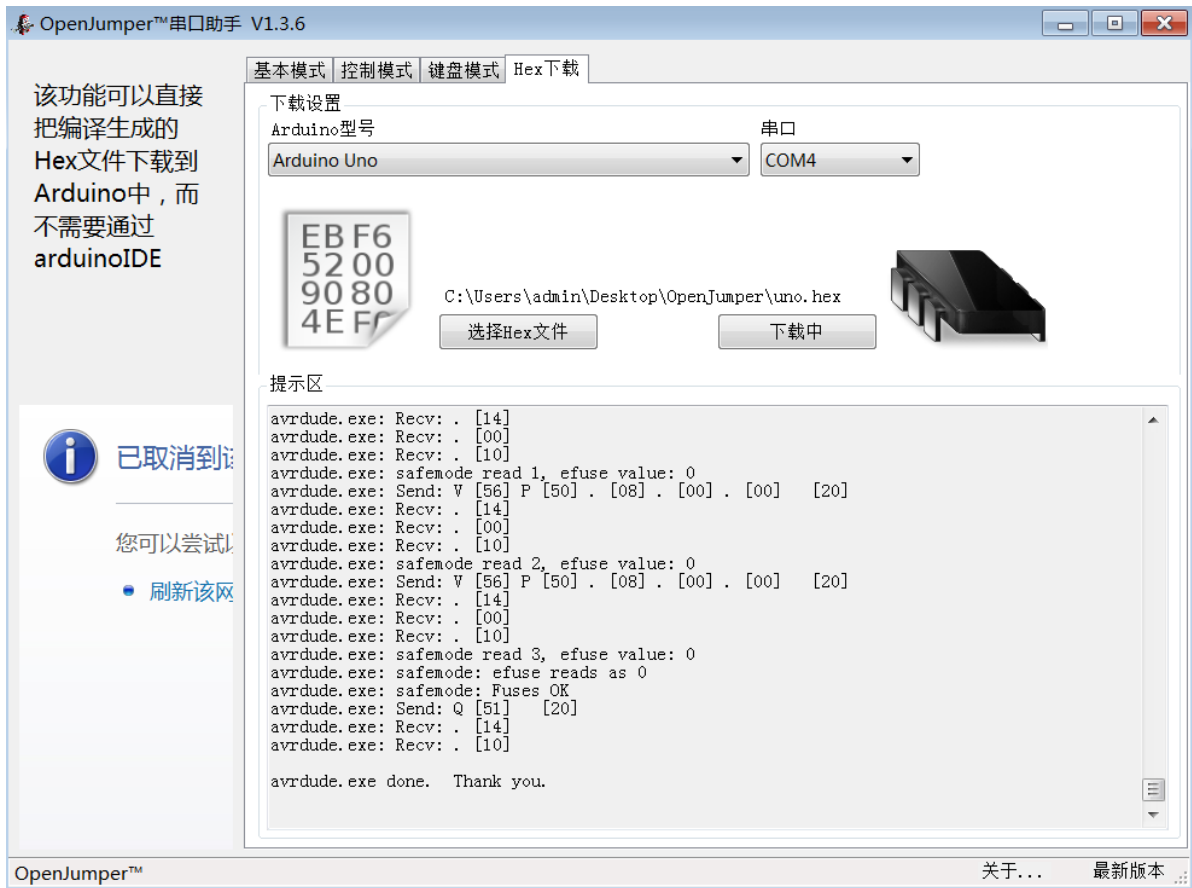
RSA Attack 3

使用 RsaCtfTool 解密。先自动探测方法，发现可以使用wiener。

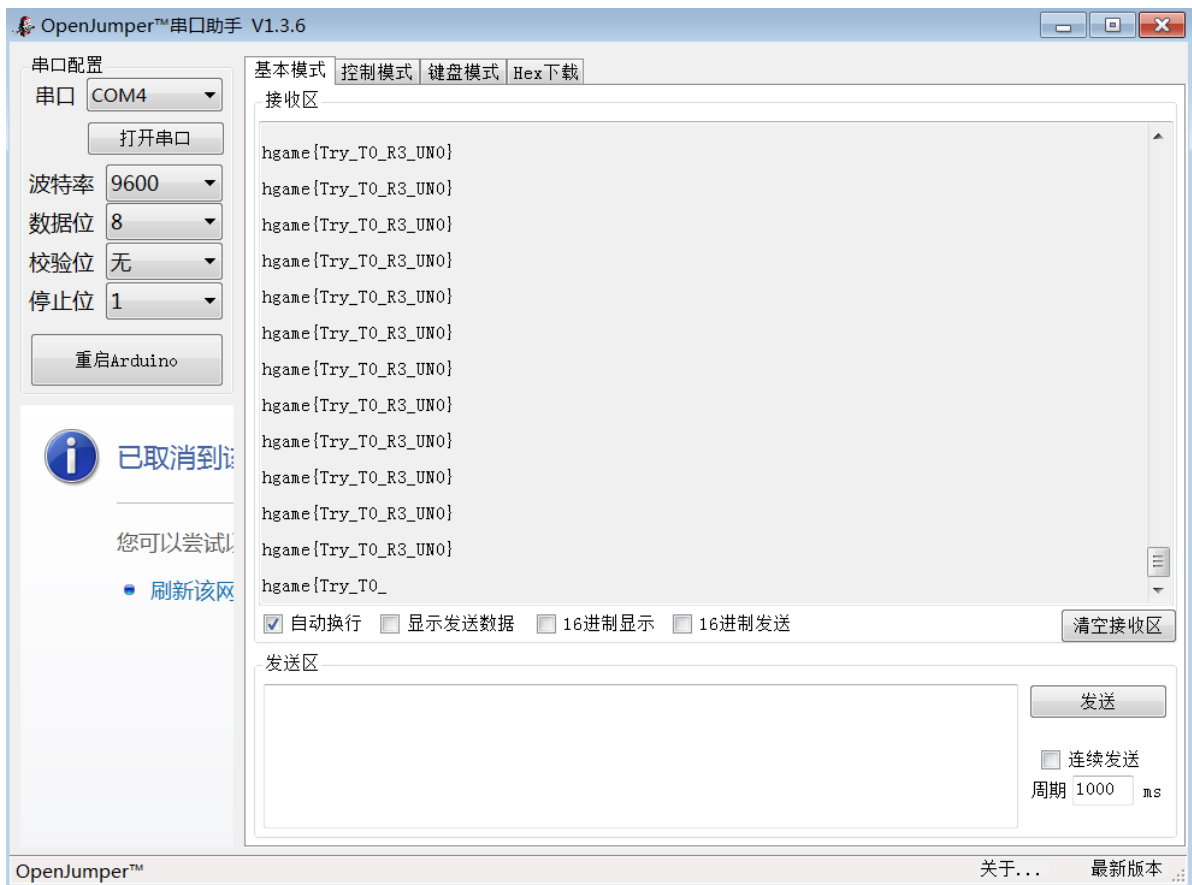
```
[*] Timeout.
[*] Performing partial_q attack on /tmp/tmp1x87a6j.
[*] Performing primordial_pm1_gcd attack on /tmp/tmp1x87a6j.
100%|████████████████████████████████████████████████████████████████████████████████| 10000/10000 [00:01<00:00, 5603.18it/s]
[*] Performing SQUFOF attack on /tmp/tmp1x87a6j.
[!] Timeout.
[*] Performing boneh_durfee attack on /tmp/tmp1x87a6j.
Can't load boneh_durfee because sage binary is not installed
[*] Performing small_crt_exp attack on /tmp/tmp1x87a6j.
Can't load small_crt_exp because sage binary is not installed
[*] Performing qicheng attack on /tmp/tmp1x87a6j.
Can't load qicheng because sage binary is not installed
[*] Performing z3_solver attack on /tmp/tmp1x87a6j.
[!] Timeout.
[*] Performing siqs attack on /tmp/tmp1x87a6j.
Can't load siqs because yafu binary is not installed
[*] Performing pollard_p_1 attack on /tmp/tmp1x87a6j.
0%|████████████████████████████████████████████████████████████████████████████████| 0/997 [00:18<?, ?it/s]
[*] Performing pisano_period attack on /tmp/tmp1x87a6j.
[*] Performing wiener attack on /tmp/tmp1x87a6j.
100%|████████████████████████████████████████████████████████████████████████████████| 1260/1260 [00:03<00:00, 318.60it/s]
3%|████████████████████████████████████████████████████████████████████████████████| 38/1260 [00:00<00:00, 2104.99it/s]
[*] Attack success with wiener method !
```

payload:

```
python3 RsaCtfTool.py -n 5074191.....759 -e 7731019.....095 --uncipher 1652517.....224 --
attack wiener
```

烧录成功后，打开串口



MISC

卡中毒

使用 AXIOM 打开 raw 文件。发现几个可疑的文件记录

Magnet AXIOM Examine v4.6.0.21968 - 202201
文件(&F) 工具 进程 帮助(&H)

过滤器 证据 使用痕迹 内容类型 日期和时间 标签和备注 配置文件 部分结果 关键字列表 肤色

所有证据 31,313
精炼信息 87
分类广告 URL 1
标识符 - 设备 7
标识符 - 人员 5
已本地访问的文件和文件夹 18
恶意软件/网络钓鱼 URL 51
已解析搜索查询 4
色情 URL 1
WEB 相关 559
Edge/Internet Explorer 10-11 主历史记录 1
Internet Explorer 缓存记录 9
Internet Explorer Cookie 记录 2
Internet Explorer 每日历史记录 23
Internet Explorer 主历史记录 25





证据 (559)
项 类型 使用... 日期和时间
file:///C:/Users/Actue/Desktop/xiaoma.zip Internet Explorer 主历史记录 Web 相关 2022/2/2 21:15
http://xz.w10a.com/small/Oem7F7.rar Internet Explorer 主历史记录 Web 相关 2022/2/2 21:16
https://www.msn.cn/?ocid=iehp Internet Explorer 主历史记录 Web 相关 2022/2/2 23:17
file:///C:/Users/Actue/Downloads/Oem7F7.rar Internet Explorer 主历史记录 Web 相关 2022/2/2 21:18
http://go.microsoft.com/fwlink/?LinkId=57426&Ext=rar Internet Explorer 主历史记录 Web 相关 2022/2/2 21:18
http://go.microsoft.com/fwlink/?LinkId=69157 Internet Explorer 主历史记录 Web 相关 2022/2/2 23:17
https://cn.bing.com/search?format=rss&form=MO0035&q=open+ra... Internet Explorer 主历史记录 Web 相关 2022/2/2 21:18
https://www.baidu.com Internet Explorer 主历史记录 Web 相关 2022/2/2 23:17
https://static-global-s-msn-com.akamaized.net/hp-eas/sc/2b/a5ea21... Internet Explorer 主历史记录 Web 相关 2022/2/2 21:16
file:///C:/Users/Actue/Desktop/flag.txt.txt.WannaRen Internet Explorer 主历史记录 Web 相关 2022/2/3 0:47
https://z6stkux-www.photoshop-com-4pbxyvfbton.fgongbi01.cn/0Lc... Internet Explorer 主历史记录 Web 相关 2022/2/2 21:19
http://dl.bandisoft.com/bandizip.std/BANDIZIP-SETUP-STD-X64.EXE?1 Internet Explorer 主历史记录 Web 相关 2022/2/2 23:16
file:///C:/Users/Actue/Desktop/flag.txt.txt.7z Internet Explorer 主历史记录 Web 相关 2022/2/2 23:16
https://www.msn.cn/zh-cn?ocid=iehp Internet Explorer 主历史记录 Web 相关 2022/2/2 23:17
http://shell.windows.com/fileassoc/fileassoc.asp?Ext=rar Internet Explorer 主历史记录 Web 相关 2022/2/2 21:18
https://www.bing.com/search?form=MO0035&q=open+r+r+file Internet Explorer 主历史记录 Web 相关 2022/2/2 21:18
http://www.winwin7.com/soft/win7jh-7928.html Internet Explorer 主历史记录 Web 相关 2022/2/2 21:19
https://cn.bing.com/search?form=MO0035&q=open+r+r+file Internet Explorer 主历史记录 Web 相关 2022/2/2 21:18

用 volatility 尝试把这几个文件提取出来。

```
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。

安装最新的 PowerShell，了解新功能和改进！ https://aka.ms/PSWindows

PS C:\Users\Halo\Downloads\CTF Tools\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone> .\volatility.exe -f .\ACTUE.raw --profile=Win7SP1x64 filescan | findstr flag
Volatility Foundation Volatility Framework 2.6
0x000000007e3c5070      2      0 RW-rw- \Device\HarddiskVolume2\Users\Actue\AppData\Roaming\Microsoft\Windows\Recent\flag.txt.txt (2).lnk
0x000000007eccc900      2      0 -W---- \Device\HarddiskVolume2\Users\Actue\Desktop\flag.txt.txt.7z
0x000000007f3e8070      2      1 R--r-- \Device\HarddiskVolume2\Users\Actue\Desktop\flag.txt.txt.7z
0x000000007f743720      1      0 R--r-- \Device\HarddiskVolume2\Users\Actue\Desktop\flag.txt.txt.WannaRen
PS C:\Users\Halo\Downloads\CTF Tools\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>
```

 binwalk	2021/2/15 15:04	文件	1 KB
 file.None.0xfffffa801b2fa8b0.dat	2022/2/3 20:42	DAT 文件	4 KB
 file.None.0xfffffa801bef02f0.zip	2022/2/3 20:41	ZIP 压缩文件	256 KB
 file.None.0xfffffa801c3c6270.dat	2022/2/3 20:41	DAT 文件	4 KB

提取出来的几个文件中，使用 binwalk 发现了其中一个压缩包文件。解压得到 flag.txt.txt.WannaRen。查询得知 wannaRen 勒索病毒。使用 火绒wannaRen专用解密工具 解密该文件，得到 flag.txt.txt

新佛曰：諸隸僧降閑呬諸陀摩閑隸僧鉢薩閑願梅願嘑願諦閑諸囉閑嗔劫嗔閑亦伏迦薩摩慙心薩摩降眾閑聞諸阿我閑嚕諸寂嘑兜咒莊閑我薩闍嚕劫閑薩摩迦聞色須嗔聞我呬伏閑是般如閑

根据经验，发现是 与佛论禅，但不完全是。检索之后找到 新约与佛论禅



hgame{F1srt_STep_0f_MeM0rY_F0renS1cs}



新佛曰：諸隸僧降閱叶諸陀摩閱隸僧鉢薩閱願禰願得願諦閱諸囉閱嚩劫嚩閱亦伏迦薩摩慙心薩摩降眾閱聞諸阿我閱嚩諸寂隔咒咒莊閱我薩闍嚩劫閱嚩薩迦聞色須嚩聞我叶伏閱是般如閱

WEB

Vidar shop demo

误打误撞，用了账号 123 密码 123，登录了某个大佬的账号，直接拿到 flag

这样不太好。研究研究怎么做吧

考点：条件竞争

一番探索后，发现 订单列表 中的 删除 居然是退款。下几个订单并付款。打开 Burp suite 的 Proxy。重复点击 删除 产生多个退款请求的包。点击关闭 Intercept，让多个请求包同时发出，其中有些订单重复退款。得到足够的余额后，正常购买得到 flag。

注：如果使用 Intruder 模块重放同一个退款请求，在第一个包后似乎有停顿，难以达到同时发出请求的效果。尝试了几次都失败了。

编号	476
性别	男
手机	halo12345
姓名	halo12345
余额	10099

注销



【Flag】 hgame{892b2d6bd236a7b3032e442a80d51b01ee26a817707570b44

¥10000.00 ¥10000.00

自营 自提

剩余 96540 件