

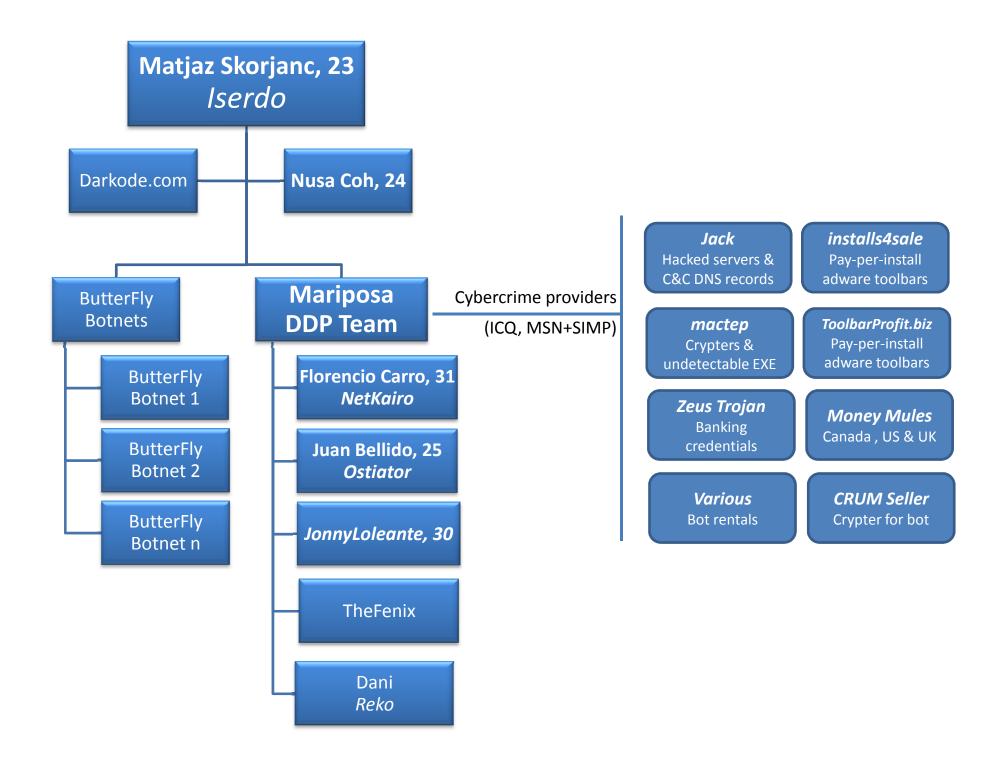
Cybercrime Files

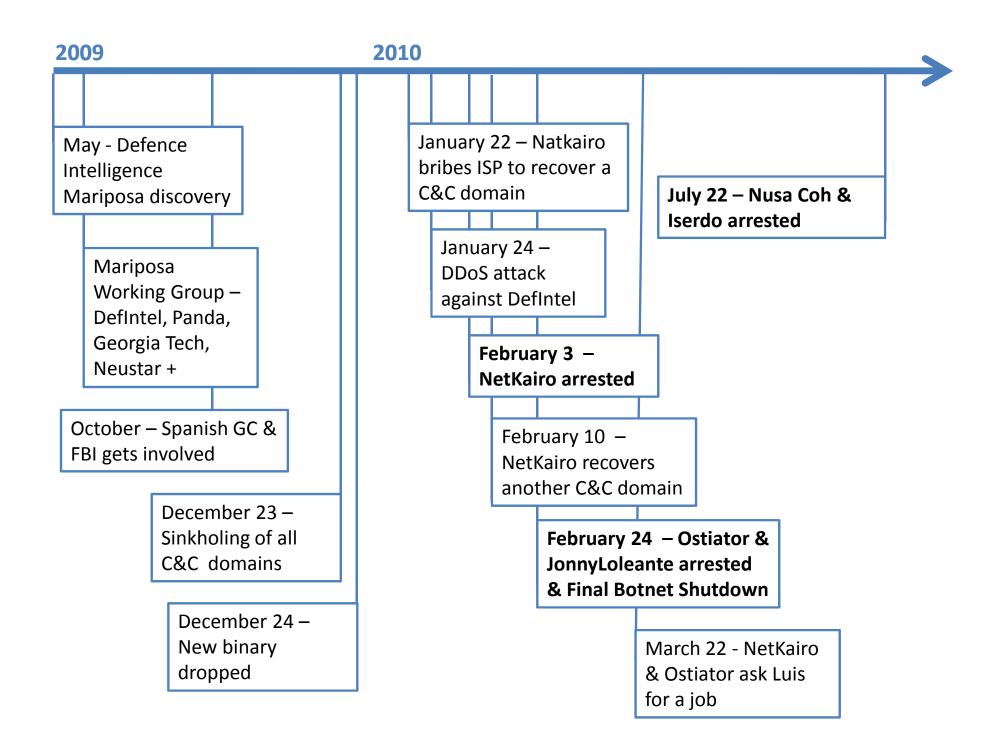
BUTTERFLY & MARIPOSA

SHUTDOWN AND ARRESTS



Pedro Bustamante, Senior Research Advisor Panda Security Virus Bulletin Vancouver 2010





Forensic Analysis

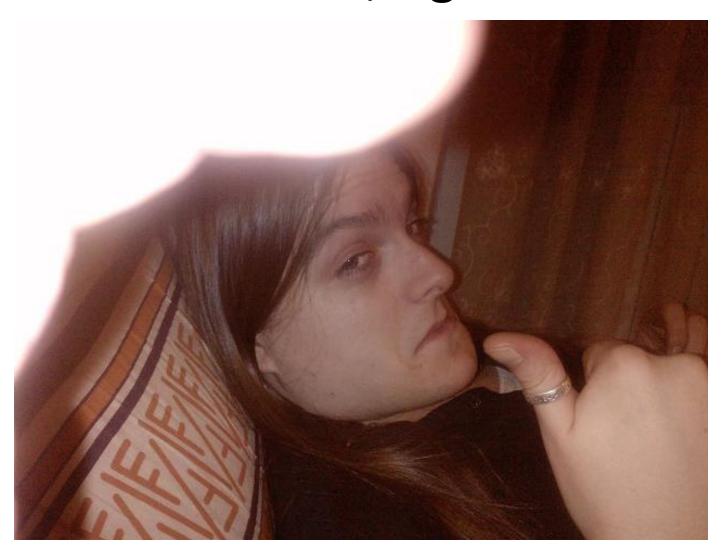
- MacBook + Win7 VM
- MacMini
- USB drive
- 2x Windows PC
- External hard drive

- Credentials to VPNs, C&Cs, WebMoney, ...
- Stolen credentials.
- Mule contacts.
- Western Union payments
- ICQ & MSN contacts & chats.
- Memory dumps from MSN.
- Cryptors, IRC bots, ...

NetKairo, Age 31



Ostiator, Age 25



JonnyLoleante, Age 30



Mariposa DDP Team



Mariposa DDP Team



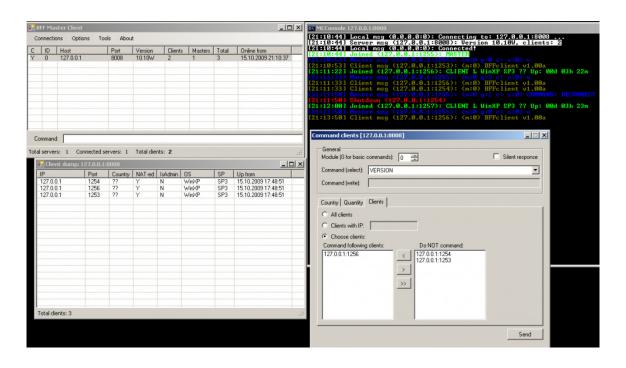
Mariposa DDP Team

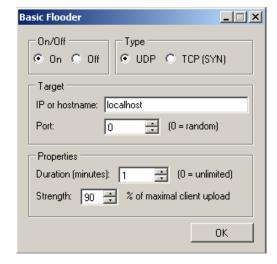


Dani aka "ReKo"









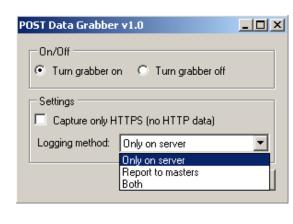
ernal Downloader v1.0		
Network settings		
URL (starts with HTTP(S) or FTP):		
http://		
User agent:		
Mozilla		
Destination		
 Save to directory for temporary 	files	
C. Save to custom directory (you u	can use environment-variable strings in form %string%]:	
1		
Generate random name (without Custom name (without extension Execute options		
Execute	Command line:	
Try to delete after execution		
Uninstall client after execution	Uninstall code: 0	
Uninstall client after execution	Uninstall code:	
	Uninstall code: 0	

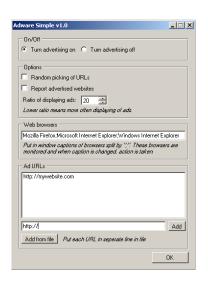
Successful Spreading Mechanism



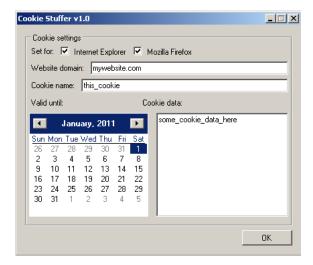


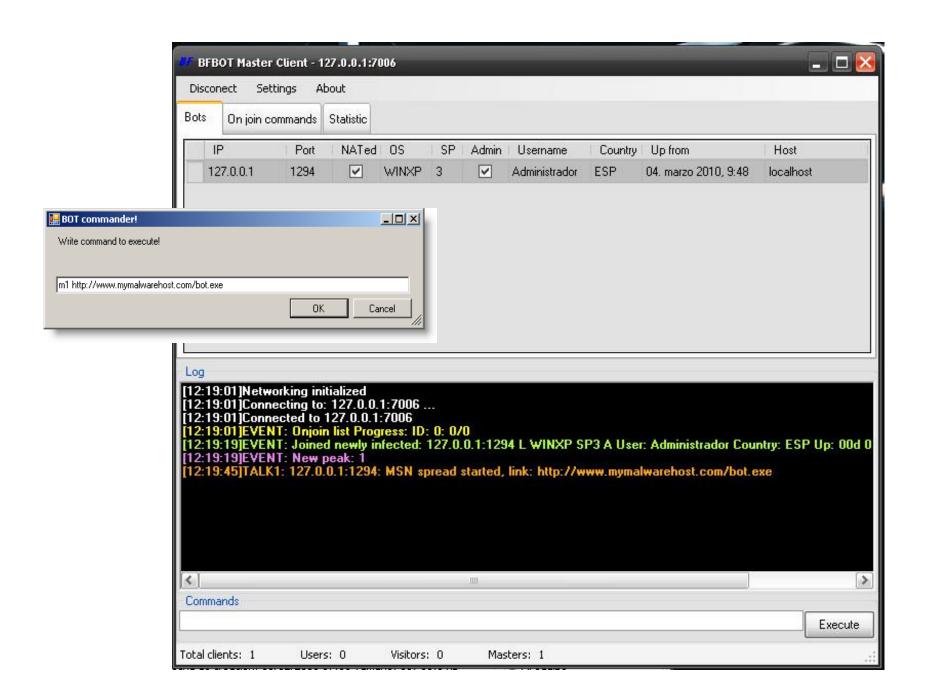












Forensic Analysis: Private Version

```
BFBot 1.0
BFBot 1.0 src
BFBot 1.2
BFBot 1.23
BFBot 1.26
BFBot 1.28
🛅 BFBot 1.28 src
BFBot 1.29
BFBot 1.29 src
BFBot 1.30 Extended
BFBot 1.30 Extended-2
BFBot 1.30 Extended-Leaked
BFBot 1.40 Pro
a BFBot 1.44 Pro -luis
 BFBot 1.46 Pro -aleii-
🛅 BFBOt 1.46 Pro -netk-
 BFBot 1.51 Pro -tenix- 1
🛅 BFBot 1.51 Pro -fenix- 3
🛅 BFBot 1.51 Pro -netk-
```

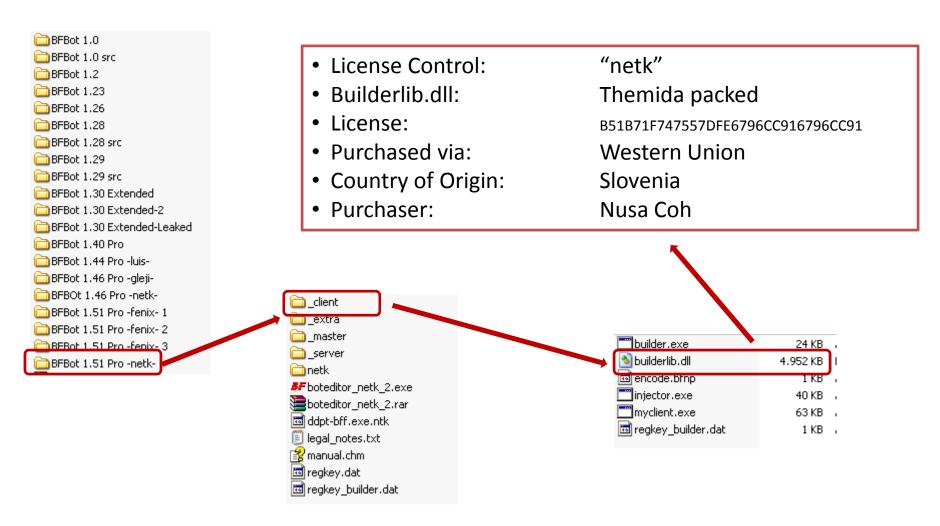
```
0012942E
          I> /8B55 F8
                                                     ; Domain integrity check
                             /MOV EDX, [LOCAL.2]
                             ADD EDX, 1
                             |MOV [LOCAL.2], EDX
          1. |8955 F8
          |> |837D F8 03
                              CMP [LOCAL.2],3
0012943B
          |. |7D 22
                             |JGE SHORT bfbot.0012945F
0012943D
          |. |8B45 FC
                             [MOV EAX, [LOCAL.1]
                             |MOV ECX, DWORD PTR DS: [EAX+34]
00129440
          I. I8B48 34
          |. |8B55 F8
                             [MOV EDX, [LOCAL.2]
00129443
00129446
          |. |8B8491 700600>|MOV EAX,DWORD PTR DS:[ECX+EDX*4+670]
0012944D
          |. |35 6E746B32
                             |XOR EAX, 326B746E
00129452
          |. |8B4D FC
                             [MOV ECX, [LOCAL.1]
                             |MOV EDX, DWORD PTR DS: [ECX]
00129455
          |. |8B11
00129457
          |. |3B02
                             |CMP EAX, DWORD PTR DS: [EDX]
          1. 175 02
                             |JNZ SHORT @@do inestable
00129459
0012945B
          1. IEB 02
                             | JMP SHORT @@check ok
```

\JMP SHORT bfbot.0012942E

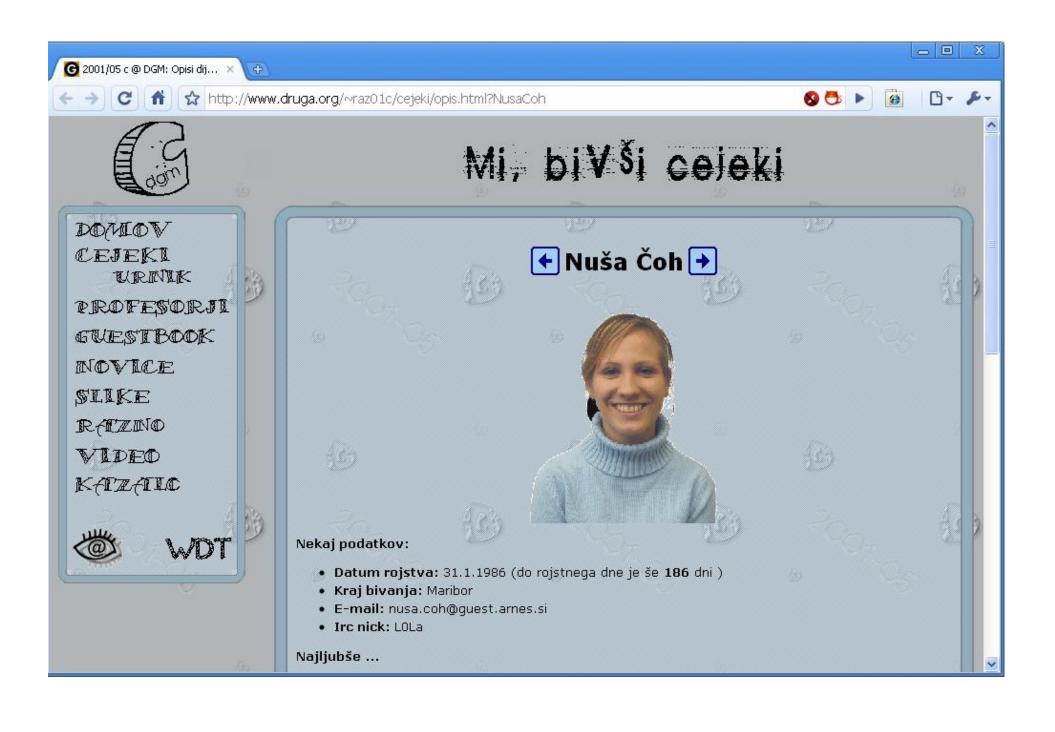
0012945D

1>^\EB CF

Forensic Analysis: Private Version







Collateral damage?



Dejan Janzekovic

Lessons learned

 Just shutting down botnet C&C's does not stop the bad guys.

 Arresting the bad guys doesn't stop them either ⁽²⁾

 Communication with law enforcement is oneway and difficult, but results are better than simple shutdowns.