Viruses in France: The French Connection – II

Francois Paget[1]
Network Associates, France

About the Author

François PAGET is a member of AVERT (Anti-Virus Emergency Response Team) inside NETWORK ASSOCIATES' McAfee Labs since 1993. In Europe, he provides virus analysis and identification, as well as removal. On request, he provides on-site expertise and data recovery in cases of complex viral infection.
François PAGET has been working on viruses since 1988 and was previously a virus and computer security expert inside the ALCATEL Group. He is a regular speaker at French computer security conferences.
In 1991, he managed the «CLUSIF Virus Group» (French Security of Information Systems CLub) which led him to be a founding member of the French RECIF Association (Researches and Studies on the French Computer Criminality) in 1992. He was President of this Association until 1994. Within RECIF, he managed the «Debug Group» which conducted technical study of the new viruses appearing in France. In the «Micro-computer Commission» of CLUSIF, he participates in the «Logical Attack Sub-Commission».
In Europe, François PAGET is an EICAR member (European Institute of Computer Anti-virus Research). Also, along with 45 other virus information professionals around the world, he is a «WILDLIST» contributor.
More recently, in September 1997, he co-founded with Marc BLANCHARD (TREND MICRO) the first INTERNET forum in French on the virus topic: TECH_VIR_F-L

Mailing Address: Network Associates, 50, rue de Londres, 75008 Paris, FRANCE; Phone: + 33 (0)1 44 90 87 46; Fax : + 33 (0)1 45 22 75 99; E-mail: francois_paget@nai.com

Descriptors

computer virus, France, malevolence, criminality, hackers

Reference to this paper should be made as follows: Paget, F. (1999) 'Viruses in France: The French Connection – II', EICAR 1999 Best Paper Proceedings.

---

[1] Please send comments and requests for remarks, adding and improvements to François Paget, Network Associates, 50, rue de Londres, 75008 Paris, France. Telephone: + 33 (0)1 44 90 87 46; Fax : + 33 (0)1 45 22 75 99; E-mail: francois_paget@nai.com

Acknowledgement
Many thanks to Jimmy Kuo (Director, Anti-Virus Research, Network Associates, USA) who has edited this paper.

Viruses in France: The French Connection – II

Abstract

This paper analyzes the computer virus situation in France. Part I was published in Virus Bulletin in August of 1997 as «The French Connection». Many things have changed since then. So playing on the idea of a movie title, I am happy to present the sequel « The French Connection - II ».

The RECIF Association (Researches and Studies on the French Computer Criminality) conducted the first serious studies on the evolution of the viral phenomenon in France at the end of 1992. Since this date many other surveys have been done. This paper will first analyze that studies in order to show the evolution of viruses in France.

First, I would like to give you an overview of the increase in computer viruses in France from 1992 to the present. I am going to talk about France but I would not be surprised if we can extend the French experience to other countries...

France was the first country to produce a virus generator. The total number of viruses that have been written in France is about 120.

Secondly, I will focus on this virus story, the individual history of different viruses, year by year, from 1988 to the present.

After that, we shall look at the various actors who have played their part in this story: virus writers, authorities and associations.

Finally I will speak about the potential implications for Decision-Makers and Researchers induced by this kind of study.

Viruses in France: The French Connection – II

Representing approximately one fifth of the European Union area, France is the largest country in Western Europe. 60 million inhabitants share 15 million microcomputers (10 million in companies and 5 million home computers).

Evolution

The RECIF Association made the first serious study concerning the evolution of the viral phenomenon in France at the end of 1992. At that time, when the number of viruses worldwide was about 2600, the total number «in the wild» in France did not exceed forty. The number has doubled in 1998.

Some viruses have been encountered only for one year. Some others are present since 1992 (Table 1). 264 various viruses have circulated in France in 7 years. (I made a mistake in the VB paper where I announced that the number was 450 viruses).
Regarding 1998, the full virus lists are available in Appendix 1 and Appendix 2.

Table 1: VIRUSES ANNOUNCED " IN-THE-WILD" – FRANCE AND WORLDWIDE

YEAR	IN-THE-WILD (FRANCE)	IN-THE-WILD (WORLDWIDE) WILDLIST – J. Wells	PARTICIPANT NUMBER WILDLIST – J Wells	TOTAL NUMBER OF VIRUS (ESTIMATION)
1992	39			2550
1993	49	67	11	4050
1994	70	92	16	5550
1995	96	190	27	8300
1996	88	212	42	12000
1997	81	267	46	14400
1998	95	257	47	25000

The stable number since 1995 is surprising while everyone thinks the phenomenon is increasing. However, I believe the reason is simple. Viruses are now quite usual and many alerts are no longer reported. Have you noticed the number of viruses in the «main list» of the Joe Wells' WILDLIST is also constant since November 1997?

There is another possible reason. Macro viruses are more and more prevalent and some anti-virus products don't mark the difference between the numerous variants. In this same way, end users often indicate only the generic name (examples: CAP, MDMA, NPAD or WAZZU) without the variant designation. Only the French variants are occasionally distinguished. 15 variants have been noticed in France by the middle of November 1998 at a time when 832 variants were known for the four virus families named before (Table 2).

Table 2: SOME MACRO-VIRUSES ANNOUNCED " IN-THE-WILD" IN FRANCE

VIRUS	REFERENCED VARIANTS IN-THE-WILD (Q3/1998 - FRANCE)	VMACRO status (Nov. 98)
CAP	A	A ==> HT
WAZZU	A, AO, DO, DV, DW, DX, EC, EY, FF, FJ, FP:FR	A ==> FN
MDMA	A	A ==> BO
NPAD	A	A ==> JC

In 1995, before the macro-virus infestation, we considered that 2% of the French microcomputers had undergone a viral attack during the year. For its part, the RECIF Association continued to log virus alerts (Table 3). In 1995, there were 400,000 machines under the responsibility of the RECIF members, for which there were 3150 alerts. The most common alert affected only 1 to 3 machines.

Table 3: VIRUS ALERTS LOGGED IN FRANCE

YEAR	NUMBER OF ALERTS
1992	410
1993	720
1994	1300
1995	3150

The collecting of this information has stopped and all these rates are overrun. The virus phenomenon is taking a worrying turn for all the French heads of companies. RECIF members indicates that 1 machine in 12 was infected in 1997 (1 in 19 in 1996). In July 1997, all the most significant companies had been confronted with CAP: it was not exceptional to find more than 8,000 infected files in one company. More surprising, in August 1998, a PE file infector (WIN32/HLLP.DeTroie.A) spread like wildfire.

Year By Year History

The number of the viruses that were written in France is near 120. For most of them, we know the creation year (Table 4). A full list is available in APPENDIX 3. Many viruses are file infectors but an increasing number of macro-viruses must be noted (Table 5).

The first French virus was E.D.V. (I don't know what it means!). Discovered in the city of Le Havre in 1988, it had been named CURSY VIRUS at first. Many days later, in January 1990, it was rediscovered under the name of E.D.V. or STEALTH VIRUS. It was one of the first viruses to effectively use a stealth technique.

Various virus encyclopedias note 3 French viruses were created in 1990 named MARDI_BROS, TCC and PARIS. These viruses seem not to be spreading much and reports are rare.

Table 4: NUMBER OF VIRUSES WRITTEN IN FRANCE

CREATION YEAR	NUMBER OF VIRUSES	TOTAL NUMBER
unknown	2	2
1988	1	3
1989		
1990	3	6
1991	3	9
1992	7	16
1993	15	31
1994	6	37
1995	21	58
1996	16	74
1997	21	95
1998	27 (Q1 to Q3)	122

Table 5: TYPE OF VIRUS WRITTEN IN FRANCE

TYPE OF VIRUS	NUMBER (1997)	NUMBER (Q3 - 1998)
FILE INFECTOR	64	68
BOOT SECTOR INFECTOR	11	11
MULTI-PARTITE	1	1
MACRO-VIRUS	3 in 1996 – 17 in 1997	42

In 1990, the first virus generator appeared. Its name was GENVIRUS. The German VCS engine had been written during this same period and many references classify it as the first. However, the Virus Research Center Karlsruhe indicated the discovery of VCS 1.0 as March of 1991. In its September 1992 edition, Virus Bulletin indicated the discovery date of 1990 without any details. And the VDAT encyclopedia cites « 1990/91 ». Some other interesting information concerning GENVIRUS and VCS are available in 40Hex Issue 10 Volume 3 Number 1. In this issue GENVIRUS was acclaimed to be first. My GENVIRUS copy is dated November 11th, 1990:

```
LISEZMOI DOC      8112 11.11.90   12:00
GV       EXE     40278 11.11.90   12:00
ELIMGVIR EXE     12252 11.11.90   12:00
MODPRN   COM       493 11.11.90   12:00
GV       DOC     67422 11.11.90   12:00
```

In May 1991, a popular computer magazine distributed to its readers an infected diskette with the Israeli FRODO virus (alias 4096). An estimated 70,000 infected diskettes were distributed. Only two companies affected by this virus lodged complaints. Two people working in the duplication firm were convicted and sentenced (Two years suspended imprisonment, 100,000-franc fine and more than 3 million francs for damages). The first trial occurred in 1994. In 1995, the verdict was overturned. Then, the French Supreme Court of Appeal in 1996

quashed the appeal and remanded the case back to trial. 8 years after the incident, the case is still open.

Up to the end of 1992, the approximately twenty French viruses did not cause great repercussions. We simply must note the file infectors from the FICHV and MALAISE families to have been written in France.

The MALAISE family has no payload action. We shall note a message inside indicating a method to stop the propagation. For instance:

```
Welcome into the virus
© 1990 by InfoViruses Laboratories
V-IVL110 (COM & EXE)
To inactivate me, just set to «*» the byte in brackets:  [#]
Next time, be more prudent!
```

FICHV.2_0 and FICHV.2_1 are destructive in March. FICHV.FEXE is destructive in April. The payload overwrites the 6 first sectors of each drive head. In the first 4 sectors, we find a repeated message:

```
****Fichv 2.1 vous a eu**
```
(*Fichv 2.1 got you*).

The first large-scale infections blamed upon French viruses were in 1993.
The less virulent ones were file infectors like:

- DUAL_GTM family (alias BEWARE and alias GREVISTE (*Striker*, in English)),
- CHAOS 3 family (alias CHAOS_YEARS),
- COM2S,
- HIDENOWT (spread via many super-markets through pre-formatted diskettes, containing an infected DE.EXE file).

CHAOS 3 has a destructive payload. It triggers randomly 3 months after initial infection. The payload overwrites the hard disk ending with the message:

```
YOUR DISK HAS BEEN DESTROYED BY THE «CHAOS YEARS» VIRUS…
ACCEPT MY SINCERE SYMPATHY !
SIGNED : THE DARK AVENGER.!
```

The first French virus to spread over the world was JUMPER.B. This unoriginal boot sector virus was discovered in the first quarter of 1993 near the city of ROUEN.

In the usual case, this virus only replicates. On slower computers, the virus activates its trigger and locks the machine by repeatedly displaying the character '∈' (epsilon). This is the reason for one of its numerous aliases (Table 6).

Table 6: JUMPER.B ALIASES

JUMPER.B	VIRESC	SILLY_BP	FRENCH_BOOT
2KB	PM5	NEUVILLE	
EPSILON	BOOT_FR	BFR	

This multiplicity of aliases has quite disrupted the French industry. Some anecdotes regarding the origins of some of the others aliases: NEUVILLE is the name of a community near the city of Rouen. VIRESC is the French abbreviation for «VIRus de l'Ecole Supérieure de Commerce» *(VIRus from the Higher School of Commerce)*.

At this time, the alerts were still scrupulously being noted and the RECIF Association was able to study the complete progress of JUMPER.B throughout the country.

During 1994 and 1995 (before macro-viruses), more than 20% of viral alerts in France were due to JUMPER.B. In fact there are now 3 variants of this virus. Two of them have disappeared; they damaged the floppy boot sector. The widespread variant has this bug corrected.

Some months later, in September of 1993, the ANTIEXE virus appeared in France. The origin of this virus is contested. VSUM indicates it was from Russia. I have no proof; but in my opinion, this boot sector virus is from Paris.

In 1994 and 1995, ANTIEXE became one of the most common viruses in France (at that time, 80% of all virus alerts concerned boot sector viruses. In fact ¾ of them were reports of JUMPER.B, ANTIEXE, FORM and PARITY_BOOT).

1994 was quiet. We only had some viruses written by a guy nicknamed TURBO POWER. They were the file infectors FAILURE, COWA-BUNGA and above all ZARMA.

COWA-BUNGA and ZARMA contain encrypted messages relating to Claudia Schiffer (this name had been spelled incorrectly in COWA-BUNGA as Schieffer). The French underground community mocked at this mistake quite a bit. But ZARMA fixed this spelling mistake!

```
COWA-BUNGA VIRUS (C) 1994 by Turbo Power
*** Claudia Schieffer Lives !!!

ZARMA-VIR by T.Power
*** Claudia Schiffer Lives !!!
```

ZARMA was also interesting because of its anti-debug techniques.

The most prolific periods were indisputably the last quarter of 1995 and Q1 of 1996 involving the WEREWOLF family of viruses. These viruses were very widespread in France because the author used numerous BBSes to spread the viruses.

The different variants all had messages stating their creation dates. Some of the variants were encrypted and some not. The last ones were polymorphic. According to messages, the first viruses were written in 1994, the last in 1996. However, they generally appeared widespread between October 1995 and March 1996.

Table 7: WEREWOLF FAMILY OF VIRUSES

WEREWOLF VARIANT (SIZE)	INTERNAL NAME AND TEXT	REMARKS	FIRST SEEN
658 (658-674 bytes)	Home Sweap Home (C) 1994-95 Werewolf	EXE	Oct. 1995
678 (678-694 bytes)	Home Sweap Home (C) 1994-95 Werewolf	EXE Crypted	Jan. 1996
684a (684-700 bytes)	CLAWS (C) 1994-95 WereWolf	EXE Crypted	Oct. 1995
684b (684-700 bytes)	FANGS (C) 1994-95 WereWolf	EXE Crypted	Oct. 1995
685a (685-701 bytes)	FANGS (C) 1994-95 WereWolf	EXE Crypted	Oct. 1995
685b (685-701 bytes)	FANGS (C) 1994-95 WereWolf	EXE Crypted	
1152	SCREAM (C) 1996 WereWolf	COM, EXE	Jan. 1996
1158	SCREAM (C) 1996 WereWolf	COM, EXE	
1168	SCREAM! (C) 1995-96 WereWolf	COM, EXE	Jul. 1996
1192	BEAST (C) 1995 WereWolf	COM prepending, EXE	
1193	BEAST (C) 1995 WereWolf	COM prepending, EXE	
1208	BEAST (C) 1995 WereWolf	COM prepending, EXE	Jan. 1996
1260	WAVE v0.9 WereWolf Advanced Viral Encryption [HOWL] (c) 1996 WereWolf		
1361a	FULL MOON (C) 1995-96 WereWolf	COM, EXE Polymorphic	Mar. 1996
1361b	FULL MOON (C) 1996 WereWolf	COM, EXE Polymorphic	Mar. 1996
1361c	FULL MOON (C) 1996 WereWolf	COM, EXE Polymorphic	
1367a	FULL MOON (C) 1995-96 WereWolf	COM, EXE Polymorphic	Jan. 1996
1367b	FULL MOON (C) 1995-96 WereWolf	COM, EXE Polymorphic	
1450	[WULF2] 1996 WereWolf	COM, EXE Polymorphic	
1500a	WULF 1996 WereWolf	COM, EXE Polymorphic	Jan. 1996
1500b	[WULF] (c) 1995-1996 WereWolf	COM, EXE Polymorphic	Dec. 1995
1500c	[WULF] (c) 1995-1996 WereWolf	COM, EXE Polymorphic	

Although far behind boot sector and macro-viruses, the WEREWOLF family of viruses (Table 7) was the most encountered file infectors in France in 1996.

They ranked 22nd in the RECIF statistics of the most prevalent viruses in France of that period.

During 1996, 2 boot sector viruses were particularly widespread in eastern France. At first, they were nicknamed GOERING. They are now known as FORM.G and FORM.N.

With a trigger date to activate on or after 1st January 1997 they now destroy the first physical sector of hard disk immediately and thus no longer spread.
Similar to other FORM viruses, these viruses also bear messages:

```
This is the Hermann GOERING Virus. Heil HITLER !
Thanks to Martin BORMANN, Joseph GOEBBELS,
Heinrich HIMMLER and Rudolf HESS.
Sieg! »
```

At first, macro viruses were often dependent on the language version of WORD. This peculiarity; along with a slow adoption of the INTERNET allowed France to dodge the new plague, for a while.

However, since January 1997, the French situation has completely turned. Macro-viruses now represent more than 70% of all virus alerts in our country. Now we seldom speak about file infectors. And the boot sector infectors have become rare.

Today, sorted by number of reports, we encounter the following viruses (Table 8):

Table 8: TOP TEN VIRUS LIST IN FRANCE (Q3/1998)

VIRUS NAME
WM/WAZZU.EC
WM/CAP
WM/WAZZU.DO
WM/INEXIST.A
WIN32/HLLP.DeTroie.A (WIN32/CHEVAL)
XF/PAIX.A
JUMPER.B
FORM.A and FORM.D
PARITY_BOOT.B
ANTIEXE.A

After a slow start (3 macro viruses created in France in 1996 and 14 in 1997), 42 macro viruses are known as having been written in France. The first one on the list is WM/CONCEPT.B:FR. It is a laboratory virus created in a French bank and never encountered in the wild.

All of these viruses are uninteresting. The most widespread are WM/APPDER.A (in Q1 1997), WM/INEXIST.A (in Q4 1997) and the family WMWAZZU.DO, DV and EC (in Q1 1998 and up to now).

WM/APPDER.A was the first French macro virus in the wild. It was also once named NTTHNTA (virus writer name) or FUNYOUR (subroutine name) when it was found in December 1996. APPDER is the name of one of the macros in the virus. This virus was designed to be destructive after 20 documents had been opened. But a typo (intentional or not) rendered it mostly harmless:

```
If WOpen$ = "20" Then                ....
            Kill "C:\DOC\*.EXE"Kill "C:\DOC\*.COM"
            Kill "C:\WINDOWS\*.EXE"
            Kill "C:\WINDOWS\SYSTEM\*.TTF"
            Kill "C:\WINDOWS\SYSTEM\*.FOT"
End If
```

WM/INEXIST.A was found in the wild in October 1997. It contains no trigger and no payload. The virus name is derived from message boxes (never displayed) indicating the possible virus presence:

```
MacroExist = - 1
'MsgBox b$ + ":" + a$ + " existe"              (exist)
MacroExist = 0
'MsgBox b$ + ":" + a$ + " inexistante"         (non-existent)
```

Uniquely of interest in WM/WAZZU.DO is that it contains the author's name, the origin and the birth date, right in its code:

```
‘     VirusMacroWord du Bureau Informatique du SIRPA
‘     Virus Anti Virus du 14 juillet 1997
‘     v0.1b – Sgt THERY – 18/07/97
```

WM/WAZZU.DV is a variant and WM/WAZZU.EC is one of the numerous corruptions generated by WORD itself.

In January 1998, a new interesting kind of macro virus for Excel appeared in the wild in France. It is XF/PAIX.A. The most interesting thing about it is that it does not contain VBA modules but is implemented entirely as cell formulas. Since no anti-virus products were looking within the formula boxes, the virus was not easily noticed. But its payload (invoked with a probability of 1%) allowed its discovery: an Excel's windows with a title filling up the screen:

```
Enfin la Paix…                                (Peace at last…)
```

Recently a virus writer nicknamed «ZeMacroKiller» created a series of stupid and destructive WORD97 viruses (Table 9). One of them was in the news on the occasion of the last World Cup. W97M/ZMK.J (alias WordCup98) displayed various dialog boxes. One of them contained the names of nine of the favored football teams and the user had to choose the champion. If the choice did not match that of the virus (random selection), any of a number of destructive payloads could be triggered.

In September 1998, ZeMacroKiller also wrote a WORD macro virus generator (ZMK98MVCK).

Finally and in closing this chapter, I must speak about WIN32/HLLP.DeTroie.A (alias WIN32/CHEVAL). Let me simply note that one should consider this virus like a combination of BACK ORIFICE and a virus. The server part of the hacking engine spreads with a virus and is installed in the target computer immediately. The engine, called SOCKET23, was distributed freely on a WEB site with no link to the underground community. It was just sheer thoughtlessness!

Never had a virus had so disturbed French industry. All the big French companies have been infected between August 1998 and October 1998. Really! After offering his own remover, the author of this dirty trick made his apologies on his WEB site.

Table 9: ZEMACROKILLER FAMILY OF VIRUSES

VIRUS	NAME FROM THE AUTHOR	VMACRO ANNOUNCEMENT
W97M/ZMK.A	Epsilon97	
W97M/ZMK.B	ZMK98FAV	
W97M/ZMK.C	GamesVirus	
W97M/ZMK.D	Multivirus2	
W97M/ZMK.E	PaixVirus97	
W97M/ZMK.F	ChessAV	
W97M/ZMK.G	CryptorV97	
W97M/ZMK.H	Anthrax	
W97M/ZMK.I	Hider98	June 98
W97M/ZMK.J	WorldCup98	June 98
W97M/ZMK.K	Multivirus4	June 98
W97M/ZMK.L	W97M.ThisDoc	August 98
W97M/ZMK.M	WNW	August 98
W97M/ZMK.N		September 98

Actors

Until now, the French virus creators seemed not well organized. This situation does not seem to be changing even though we know that some French guys are in the 29A or SLAM group. The title of my first paper «The French Connection», gave an idea of criminal organization. I know that this idea displeased some virus writers who consider that the underground community is not organized in France. Effectively! I agree.

But what is really disquieting is; an investigative reporter announced to me that there were more than 70 French virus writers. This was the total number, counting current and past authors, real writers or simple «mutators» having modified only one byte in an existing virus.

For myself, I have no list and no address book. In this paper I reference less than 6 virus writers using their nicknames. I do not know how many people are hidden behind these nicknames. Moreover my full list is poor (Table 10):

It is not possible to finish this story without talking about SPANSKA. Behind this pseudonym lives the most well known French virus writer. Some of his viruses

are on the WILDLIST but are no longer widely encountered. These viruses are disturbing but not dangerous. Depending on the system time, they display texts and graphic effects (Table 11).

Table 10: SOME FRENCH VIRUS AUTHORS

PSEUDOS	GROUPS	ACTIVITY YEAR(S)
AURODREPH	SLAM	1996-1998
DJM		1993
JCZIC		July 1998 - only
KAWIK		
MISTERMAD		1996-1997
OMY L'ARCHITECTE		
SPANSKA	29A	1996-1998
THE DARK AVENGER		1993
TURBO-POWER		1995
UNK MNEMONIC	MJ13	
WEREWOLF		1995-1996
ZEMACROKILLER	SOS	1997-1998

Even though virus writing in France is not considered reprehensible, French authorities take close interest in the virus phenomenon. Both services inside the Criminal Investigation Department (Police Judiciaire) have the ability to address the problem (BCRCI and SEFTI). The Home Office also has a virus specialist section inside the DST Department (Directorate for Surveillance of the Territory). There are laws but complaints must be lodged in order to start any prosecution. Many virus writers are actually known but are not disturbed!

On the good side, two French Associations have gathered the principals in this field. Already mentioned, RECIF is only interested in Computer Malevolence. French anti-virus specialists including the Computer Security Managers from big French companies and Ministries are in RECIF.

CLUSIF takes an interest in all areas of computer security. The group has approximately 270 members comprising of distributors, providers of service and Security product manufacturers. In this Association, the Logical Attack Commission has jurisdiction on the virus subject.

On the worldwide level, anti-virus researchers are grouped in various institutions (EICAR, CARO, WILDLIST, VMACRO and VFORUM...). There are not many French people involved in this common effort. Apart from myself, I know of only one other person. He is a WILDLIST contributor.

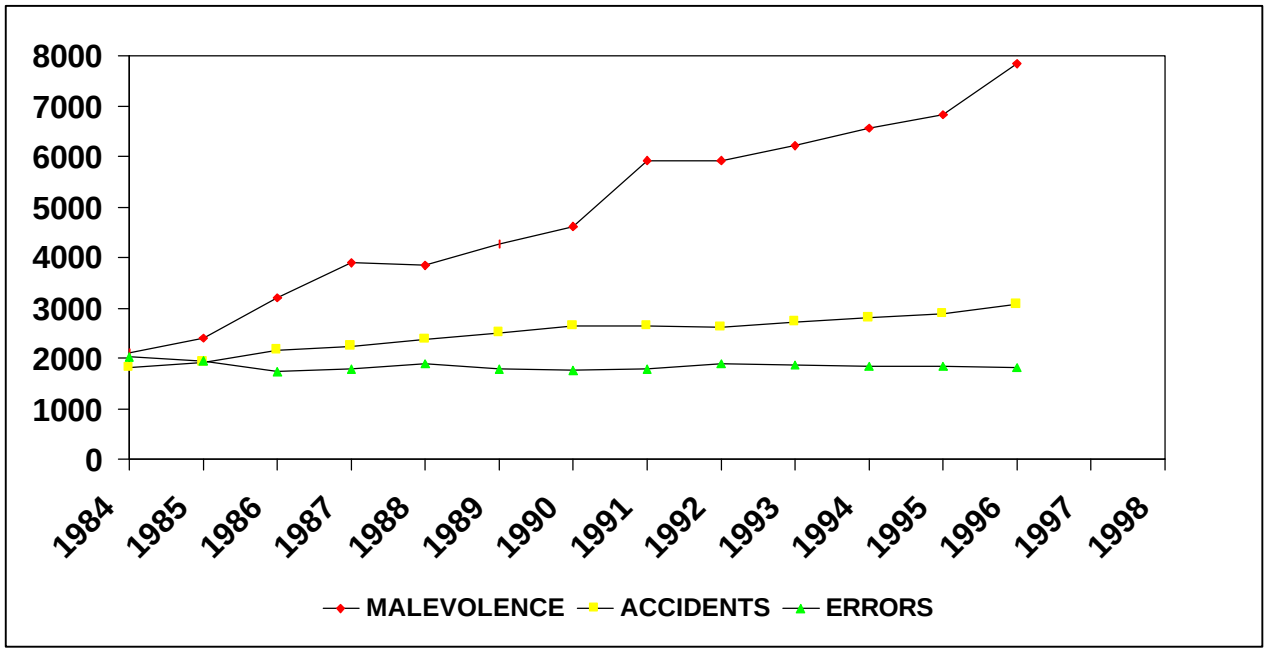
Table 11: SPANSKA FAMILY OF VIRUSES

VIRUS NAME SIZE (BYTES)	ANNOUNCED	TEXT/ANIMATION	ACTIVATION
NO PASARAN (1120 bytes)	Jan-1997	Remember those who died for Madrid No Pasaran! Virus (c) Spanska 1996 Animation of flames	
NO PASARAN (1000/1008 bytes)	1997	Remember those who died for Madrid No Pasaran! Virus v2 by Spanska 1997 Animation of flames	Minutes at 22
COSMOS (1120 bytes)	1997	To Carl Sagan, poet and Scientist,this little Cosmos. (Spanska 97) Starry sky background	
MARSLAND (1509 bytes)	Apr-1997	Mars Land, by Spanska (coding a virus can be creative) Animation of a rolling « Martian » red landscape	Minutes at 30
ELVIRA (4250 bytes)	Sep-1997	ELVIRA ! Black and White Girl from Paris You make me feel alive. ELVIRA ! Pars. Reviens. Respire. Puis repars. J'aime ton mouvement. ELVIRA ! Bruja con ojos verdes Eres un grito de vida, un canto de libertad.	Minutes at 30 and seconds less or equal than 15
IDEA (6126 bytes)	Apr-1998	Warning! strong crypto inside Rotated message	Minutes at 30 and seconds less or equal than 15

Conclusion

For 14 years, the CLUSIF statistics have shown a continuous increase of malevolence (Figure 1 : scale is in million Francs).

Figure 1 : LOSSES INDUCED BY INFORMATION TECHNOLOGY (FRANCE).



In 1996, malevolence caused 62% of the computer disasters in France (24% was attributed to accidents and 14% to errors). The frequency of virus reports is still increasing but the consequences are better controlled than in the past. Not many deliberate software attacks have been reported.

For the future, this Association predicts an increase of malevolence. Among the reasons for this opinion:

- The continuing worldwide economic crisis.
- The destabilization of some computing rules.
- The increasing levels of anti-social behavior by some segments of society.
- Finally, just the sheer number of people with access to computers and the INTERNET. This inevitably means that there is more possibility for mischief!

For concluding this paper, I must encourage other researchers to do similar studies on their local virus scene. The "local" virus situation may not be well represented by just looking at the "worldwide" virus situation. Among many others, this fact must induce implications for System Experts and Researchers around the world.

Users in France, or those who conduct business with company offices in France, need to look especially for the viruses listed or discussed, even if they are not as prevalent on the worldwide "in-the-wild" list.
As I said before, we have in France our own "Top Ten" virus list (Table 8). What surprised me, when I prepared this list, was that 7 viruses in 10 are French (Table 12).

Without similar studies, we cannot know if this fact is unique. But the preponderance of «local» viruses (from the field) in a particular country must be seriously considered.

Table 12 : VIRUS ORIGIN OF THE "TOP TEN" LIST IN FRANCE (end 1998)

VIRUS NAME	ORIGIN
WM/WAZZU.EC	FRANCE
WM/CAP	
WM/WAZZU.DO	FRANCE
WM/INEXIST.A	FRANCE
WIN32/HLLP.DeTroie.A (WIN32/CHEVAL)	FRANCE
XF/PAIX.A	FRANCE
JUMPER.B	FRANCE
FORM.A and FORM.D	
PARITY_BOOT.B	
ANTIEXE.A	FRANCE

Also, France is now more and more a participant in the worldwide "virus" scene. Previously, France had been isolated and more immune. That is no more.
Notice that more and more companies are placing researchers in "local" places. More companies are going to need an active French researcher, both to handle the French viruses, as well as to handle the "increased business" due to the increased infection rate.

APPENDIX 1

VIRUSES IN-THE-WILD IN FRANCE IN 1998
(CLASSIFIED BY FREQUENCY OF ALERTS[2])

Freq.	VIRUS NAME	ALIAS	TYPE
14	WM/WAZZU.EC	SERGENT THERY	WM-DOC
13	WM/CAP.A		WM-DOC
12	WM/WAZZU.DO	SERGENT THERY	WM-DOC
11	WM/INEXIST.A		WM-DOC
10	WIN32/HLLP.DeTroie.A	WIN32/CHEVAL.TCV	W32-PRG
9	XF.PAIX.A		XF-XLS
8	JUMPER.B	2KB, BOOT_FR, VIRESC, NEUVILLE...	MBR
7	FORM.A	BEDOT, FORM18	BOOT
7	FORM.D	BEDOT, FORM MAY	BOOT
6	PARITY_BOOT.B	GENERIC 1	MBR
5	ANTIEXE.A	D3, NEWBUG, CMOS4	MBR
4	WM/NPAD.A	JAKARTA	WM-DOC
4	WM/WAZZU.A		WM-DOC
4	XM/LAROUX.A		XM-XLS
3	ANTICMOS.A	LENART	MBR
3	ANTICMOS.B	LIXI	MBR
3	EMPIRE.MONKEY.A	MONKEY	MBR
3	EMPIRE.MONKEY.B	MONKEY 2	MBR
3	INT-AA	GNU	MBR
3	ONE_HALF.mp.3544.A	DIS, FREE LOVE	BIV-M
3	WM/APPDER.A	NTTHNTA, FUNYOUR	WM-DOC
3	WM/CONCEPT.A	PRANK MACRO	WM-DOC
3	WM/MDMA.A	STICKYKEYS	WM-DOC
2	BARROTES.1310.A	BARROTOS	PRG
2	BLEAH.A	SACK, ECO, ARMANDA, BOOT0197	MBR
2	ECO.B	BLEAH.B	MBR
2	FLIP.mp.2153.A	OMICRON	BIV-M
2	JUNKIE.mp.1027.A	JINGLE_BOOT	BIV-M
2	KAMPANA.mp.A	A-VIR, TELECOM BOOT, ANTITEL, CAMPANA	BIV-M
2	NOVEMBER_17TH.800.A	JAN1, INT83.800, 800	PRG
2	RIPPER	JACK RIPPER	MBR
2	SAMPO	69, TURBO, WLLOP	MBR
2	STONED.SPIRIT		MBR
2	TEQUILA.2468.mp.A		BIV-M
2	W95/HPS.5124		W95-PRG
2	WM/BANDUNG.A	CONCEPT.J, TEDI	WM-DOC
2	WM/SHOWOFF.A		WM-DOC
2	WM/WAZZU.DV		WM-DOC
2	ZARMA		PRG
1	BACHKHOA.3999	DUBUG.3999	PRG
1	DIE_HARD.4000.A	DH2, HDH2, WIX	PRG
1	DODGY		MBR
1	HLLP.7299	IRAQ.7299	PRG
1	JERUSALEM.1808.STANDAR	1808, 1813, ISRAELI	PRG
1	LAVOT.D		MBR
1	QUANDARY	PARITY_BOOT.ENC	MBR
1	SPANSKA.4250.A	SPANSKA_2, ELVIRA	PRG
1	STONED.ANGELINA		MBR
1	STONED.NO_INT.A	BLOOMINGTON, STONED_3	MBR

[2] Frequencies noted from 14 to 5 concern viruses inside the French « TOP 10 » list. Frequencies noted 4 to 0 concern viruses having a lower presence. Generally, frequency 0 is not noted in the J. WELLS WILDLIST.

APPENDIX 1 (CONTINUED)

Freq.	VIRUS NAME	ALIAS	TYPE
1	UNASHAMED.B		MBR
1	W95/ANXIETY.1358	POPPY, W95/ANXIETY.A	W95-PRG
1	W95/ANXIETY.1823	W95/ANXIETY.B	W95-PRG
1	W97M/TWNO.AC		WM-DOC
1	WELCOMB	BUPTBOOT,BUPT9146,BEIJING	MBR
1	WIN32/CIH.SPACEFILLER		W32-PRG
1	WM/APPDER.V		WM-DOC
1	WM/DIVINA.A	INFECZIONE	WM-DOC
1	WM/IMPOSTER.E		WM-DOC
1	WM/MENTAL.A	XM/COLORS.CE	WM-DOC
1	WM/MENTES.A		WM-DOC
1	WM/NEWYEAR.A		WM-DOC
1	WM/RAPI.A		WM-DOC
1	WM/STALL.A		WM-DOC
1	WM/SWLABS.G		WM-DOC
1	WM/TWNO.AC		WM-DOC
1	WM/WAZZU.C		WM-DOC
1	XM/LAROUX.AD		XM-XLS
1	XM/LAROUX.AJ		XM-XLS
0	BOOT-437.A	BATH	BOOT
0	CASCADE.1701.A	1701	PRG
0	EXE_BUG.A	CMOS KILLER, SWISS	MBR
0	J&M.A	JIMI, HASITA	MBR
0	KEYPRESS.1232.A	TURKU, TWINS	PRG
0	STONED.MICHELANGELO.D		MBR
0	TAI-PAN.438.A	WHISPER	PRG
0	W97M/GODZILLA.A:FR		WM-DOC
0	W97M/ZMK.J	WORLDCUP98	WM-DOC
0	WM/APPDER.R		WM-DOC
0	WM/COLORS.A	COLOURS	WM-DOC
0	WM/ELOHIM.A:FR		WM-DOC
0	WM/KILLLUF.B		WM-DOC
0	WM/KILLUF.A		WM-DOC
0	WM/KILLUF.B		WM-DOC
0	WM/LUNCH.A		WM-DOC
0	WM/NF.A		WM-DOC
0	WM/NICEDAY.X		WM-DOC
0	WM/NOP.A:DE	NOP	WM-DOC
0	WM/PANZER.A		WM-DOC
0	WM/WAZZU.AO		WM-DOC
0	WM/WAZZU.DW		WM-DOC
0	WM/WAZZU.DX		WM-DOC
0	WM/WAZZU.EY		WM-DOC
0	WM/WAZZU.FF		WM-DOC
0	WM/WAZZU.FJ		WM-DOC
0	WM/WAZZU.FP:FR		WM-DOC
0	XF.PAIX.B		XF-XLS

TYPE		
	BIV-M	Multipartite virus
	BOOT	Boot sector infector (BOOT)
	MBR	Boot sector infector (MBR)
	PRG	File infector (appending)
	PRG_R	File infector (overwriting)
	W32-PRG	File infector (PE – WIN32)
	W95-PRG	File infector (PE – WIN95)
	WM-DOC	Macro-virus (Word)
	XF-XLS	Macro-virus (Excel formulae)
	XM-XLS	Macro-virus (Excel)

APPENDIX N°2

VIRUSES IN-THE-WILD IN FRANCE IN 1998
(CLASSIFIED BY NAME[3])

Freq.	NAME VIRUS	ALIAS	TYPE
3	ANTICMOS.A	LENART	MBR
3	ANTICMOS.B	LIXI	MBR
5	ANTIEXE.A	D3, NEWBUG, CMOS4	MBR
1	BACHKHOA.3999	DUBUG.3999	PRG
2	BARROTES.1310.A	BARROTOS	PRG
2	BLEAH.A	SACK, ECO, ARMANDA, BOOT0197	MBR
0	BOOT-437.A	BATH	BOOT
0	CASCADE.1701.A	1701	PRG
1	DIE_HARD.4000.A	DH2, HDH2, WIX	PRG
1	DODGY		MBR
2	ECO.B	BLEAH.B	MBR
3	EMPIRE.MONKEY.A	MONKEY	MBR
3	EMPIRE.MONKEY.B	MONKEY 2	MBR
0	EXE_BUG.A	CMOS KILLER, SWISS	MBR
2	FLIP.mp.2153.A	OMICRON	BIV-M
7	FORM.A	BEDOT, FORM18	BOOT
7	FORM.D	BEDOT, FORM MAY	BOOT
1	HLLP.7299	IRAQ.7299	PRG
3	INT-AA	GNU	MBR
0	J&M.A	JIMI, HASITA	MBR
1	JERUSALEM.1808.STANDAR	1808, 1813, ISRAELI	PRG
8	JUMPER.B	2KB, BOOT_FR, VIRESC, NEUVILLE...	MBR
2	JUNKIE.mp.1027.A	JINGLE_BOOT	BIV-M
2	KAMPANA.mp.A	A-VIR, TELECOM BOOT, ANTITEL, CAMPANA	BIV-M
0	KEYPRESS.1232.A	TURKU, TWINS	PRG
1	LAVOT.D		MBR
2	NOVEMBER_17TH.800.A	JAN1, INT83.800, 800	PRG
3	ONE_HALF.mp.3544.A	DIS, FREE LOVE	BIV-M
6	PARITY_BOOT.B	GENERIC 1	MBR
1	QUANDARY	PARITY_BOOT.ENC	MBR
2	RIPPER	JACK RIPPER	MBR
2	SAMPO	69, TURBO, WLLOP	MBR
1	SPANSKA.4250.A	SPANSKA_2, ELVIRA	PRG
1	STONED.ANGELINA		MBR
0	STONED.MICHELANGELO.D		MBR
1	STONED.NO_INT.A	BLOOMINGTON, STONED_3	MBR
2	STONED.SPIRIT		MBR
0	TAI-PAN.438.A	WHISPER	PRG
2	TEQUILA.2468.mp.A		BIV-M
1	UNASHAMED.B		MBR
1	W95/ANXIETY.1358	POPPY, W95/ANXIETY.A	W95-PRG
1	W95/ANXIETY.1823	W95/ANXIETY.B	W95-PRG
2	W95/HPS.5124		W95-PRG
0	W97M/GODZILLA.A:FR		WM-DOC
1	W97M/TWNO.AC		WM-DOC
0	W97M/ZMK.J	WORLDCUP98	WM-DOC
1	WELCOMB	BUPTBOOT,BUPT9146,BEIJING	MBR
1	WIN32/CIH.SPACEFILLER		W32-PRG
10	WIN32/HLLP.DeTroie.A	WIN32/CHEVAL.TCV	W32-PRG

[3] Frequencies noted from 14 to 5 concern viruses inside the French « TOP 10 » list. Frequencies noted 4 to 0 concern viruses having a lower presence. Generally, frequency 0 is not noted in the J. WELLS WILDLIST.

APPENDIX N°2 (CONTINUED)

Freq.	VIRUS NAME	ALIAS	TYPE
3	WM/APPDER.A	NTTHNTA, FUNYOUR	WM-DOC
0	WM/APPDER.R		WM-DOC
1	WM/APPDER.V		WM-DOC
2	WM/BANDUNG.A	CONCEPT.J, TEDI	WM-DOC
13	WM/CAP.A		WM-DOC
0	WM/COLORS.A	COLOURS	WM-DOC
3	WM/CONCEPT.A	PRANK MACRO	WM-DOC
1	WM/DIVINA.A	INFECZIONE	WM-DOC
0	WM/ELOHIM.A:FR		WM-DOC
1	WM/IMPOSTER.E		WM-DOC
11	WM/INEXIST.A		WM-DOC
0	WM/KILLLUF.B		WM-DOC
0	WM/KILLUF.A		WM-DOC
0	WM/KILLUF.B		WM-DOC
0	WM/LUNCH.A		WM-DOC
3	WM/MDMA.A	STICKYKEYS	WM-DOC
1	WM/MENTAL.A	XM/COLORS.CE	WM-DOC
1	WM/MENTES.A		WM-DOC
1	WM/NEWYEAR.A		WM-DOC
0	WM/NF.A		WM-DOC
0	WM/NICEDAY.X		WM-DOC
0	WM/NOP.A:DE	NOP	WM-DOC
4	WM/NPAD.A	JAKARTA	WM-DOC
0	WM/PANZER.A		WM-DOC
1	WM/RAPI.A		WM-DOC
2	WM/SHOWOFF.A		WM-DOC
1	WM/STALL.A		WM-DOC
1	WM/SWLABS.G		WM-DOC
1	WM/TWNO.AC		WM-DOC
4	WM/WAZZU.A		WM-DOC
0	WM/WAZZU.AO		WM-DOC
1	WM/WAZZU.C		WM-DOC
12	WM/WAZZU.DO	SERGENT THERY	WM-DOC
2	WM/WAZZU.DV		WM-DOC
0	WM/WAZZU.DW		WM-DOC
0	WM/WAZZU.DX		WM-DOC
14	WM/WAZZU.EC	SERGENT THERY	WM-DOC
0	WM/WAZZU.EY		WM-DOC
0	WM/WAZZU.FF		WM-DOC
0	WM/WAZZU.FJ		WM-DOC
0	WM/WAZZU.FP:FR		WM-DOC
9	XF.PAIX.A		XF-XLS
0	XF.PAIX.B		XF-XLS
4	XM/LAROUX.A		XM-XLS
1	XM/LAROUX.AD		XM-XLS
1	XM/LAROUX.AJ		XM-XLS
2	ZARMA		PRG

TYPE		
	BIV-M	Multipartite virus
	BOOT	Boot sector infector (BOOT)
	MBR	Boot sector infector (MBR)
	PRG	File infector (appending)
	PRG_R	File infector (overwriting)
	W32-PRG	File infector (PE – WIN32)
	W95-PRG	File infector (PE – WIN95)
	WM-DOC	Macro-virus (Word)
	XF-XLS	Macro-virus (Excel formulae)
	XM-XLS	Macro-virus (Excel)

APPENDIX 3

FRENCH VIRUSES
(CLASSIFIED BY NAME)

VIRUS NAME	ALIAS	TYPE	!!!	SIZE	YEAR	PSEUDO
_354		PRG	X	354		
_727	FRENCH_BUG_GREVISTE	PRG	N	727	1993	DJM
ANTIEXE		MBR	X		1993	
CASCADE-1704G		PRG	N	1704	1993	
CHAOS_YEARS.1837		PRG	D	1837	1993	THE DARK AVENGER
CHAOS_YEARS.2005		PRG	D	2005	1993	THE DARK AVENGER
COM2S		PRG		1798	1993	
COWA-BUNGA		PRG		2297	1994	TURBO POWER
DUAL_GTM.1446	GANEU	PRG	N	1446	1993	DJM
DUAL_GTM.1528	FRENCH_BUG_BEWARE	PRG	N	1528 - 1544	1993	DJM
EDV	CURSY, STEALTH VIRUS	MBR	D		1988	
FACE.2521	BAK	PRG	N	2521	1992	
FAILLURE	TV-II,	PRG	N	1366	1994	TURBO POWER
FICH-C		PRG	D		1991	
FICHV_2.0	FICHV_896	PRG	D	896	1992	
FICHV_2.1	FICH, FICHV, 903	PRG	D	903	1991	
FICHV_EXE_1.0	FICH_897	PRG	D	897	1992	
FORM_G	GOERING_A	BOOT	D		1995	
FORM_L		BOOT	N		1996	
FORM_N	GOERING_B	BOOT	D		1996	
HIDENOWT	MALAISE-1743	PRG	N	1743 - 1757	1993	
JUMPER-A	BFR	MBR	N		1993	
JUMPER-B (EA 05)	2KB, BOOT_FR	MBR	N		1993	
JUMPER-B (EB 01)	2KB, BOOT_FR	MBR	N		1993	
LAVOT		MBR			1997	
LOKI_1237	MERDE	PRG	X	1237		
MALAISE	V-IVL110	PRG	N	1357 - 1371	1992	
MALAISE-524	LOCKS	PRG	N	524	1993	
MALAISE-B		PRG	N	1357 - 1371	1992	
MARDI BROS		BOOT	N		1990	
MJ13.80/86		PRG_R	D	80 or 86	1997	GROUPE MJ13
MONAMI		PRG		1059	1995	
NMANU.4096		PRG	N	4096	1994	
PARIS		PRG	X	4909 - 4925	1990	
PITCH		PRG	X	593	1992	
PITCH-B		PRG	X	593	1992	
RODOLF		PRG	N	4096	1993	
SADDAM		PRG	N	919	1991	
SAURON		PRG	N	1088	1993	
SCOTCH_2611		PRG	N	2611	1995	
SKYNET.1809	ENCULATOR_III	PRG	N	1809	1994	TURBO POWER ?
SPANSKA.1000	NO_PASARAN (1996)	PRG		1000	1997	SPANSKA
SPANSKA.1120	NO_PASARAN (1997)	PRG		1120	1997	SPANSKA
SPANSKA.1120B	COSMOS	PRG		1120	1997	SPANSKA
SPANSKA.1500	MARS_LAND	PRG		1500	1997	SPANSKA
SPANSKA.4250	SPANSKA_2, ELVIRA	PRG		4250	1997	SPANSKA
SPANSKA.6126		PRG		6126	1998	SPANSKA
SPHINX_2751		BIV-M		2751	1995	

APPENDIX 3 (CONTINUED)

VIRUS NAME	ALIAS	TYPE	!!!	SIZE	YEAR	PSEUDO
SURIV 2.01B		PRG		1488	1994	
TCC	4909	PRG			1990	
TIMID_298		PRG	X	292	1995	
TRIVIAL.111	NATIONAL	PRG_R	N	(111)	1995	
TVC3		PRG			1998	
UGLY-JO		MBR	N		1996	
UNKNOWN1.0	UNKNOWN1.1111	PRG	D		1995	
UNKNOWN1.1	UNKNOWN1.1279	PRG	D		1995	
W97M.CASC.A		WM-DOC			1998	ZEMACROKILLER ??
W97M.GODZILLA.A:FR		WM-DOC			1998	
W97M.ZMK.A	EPSILON97	WM-DOC	D		1997	ZEMACROKILLER
W97M.ZMK.B	ZMK98FAV	WM-DOC	D		1998	ZEMACROKILLER
W97M.ZMK.C	GAMEVIRUS	WM-DOC	D		1998	ZEMACROKILLER
W97M.ZMK.D	MULTIVIRUS2	WM-DOC	D		1998	ZEMACROKILLER
W97M.ZMK.E	PAIXVIRUS97	WM-DOC	D		1997	ZEMACROKILLER
W97M.ZMK.F	CHESSAV	WM-DOC	D		1998	ZEMACROKILLER
W97M.ZMK.G	CRYPTORV97	WM-DOC	D		1997	ZEMACROKILLER
W97M.ZMK.H	ANTHRAX	WM-DOC	D		1998	ZEMACROKILLER
W97M.ZMK.I	HIDER98	WM-DOC	D		1998	ZEMACROKILLER
W97M.ZMK.J	WORLDCUP98	WM-DOC	D		1998	ZEMACROKILLER
W97M.ZMK.K	MULTIVIRUS4	WM-DOC	D		1998	ZEMACROKILLER
W97M.ZMK.L	W97M.THISDOC	WM-DOC	D		1998	ZEMACROKILLER
W97M.ZMK.M	WNW	WM-DOC	D		1998	ZEMACROKILLER
W97M.ZMK.N		WM-DOC	D		1998	ZEMACROKILLER
WEREWOLF.1152	SCREAM	PRG	N	1152	1996	WEREWOLF
WEREWOLF.1158	SCREAM	PRG	N	1158	1996	WEREWOLF
WEREWOLF.1168	SCREAM!	PRG	N	1168	1995	WEREWOLF
WEREWOLF.1192	BEAST	PRG	N	1192	1995	WEREWOLF
WEREWOLF.1193	BEAST	PRG	N	1193	1995	WEREWOLF
WEREWOLF.1208	BEAST	PRG	N	1208	1995	WEREWOLF
WEREWOLF.1260	HOWL	PRG	N	1260	1996	WEREWOLF
WEREWOLF.1361a	FULL MOON	PRG	N	1361	1996	WEREWOLF
WEREWOLF.1361b	FULL MOON	PRG	N	1361	1996	WEREWOLF
WEREWOLF.1361c	FULL MOON	PRG	N	1361	1996	WEREWOLF
WEREWOLF.1367a	FULL MOON	PRG	N	1367	1996	WEREWOLF
WEREWOLF.1367b	FULL MOON	PRG	N	1367	1996	WEREWOLF
WEREWOLF.1450	[WULF2]	PRG	N	1450	1996	WEREWOLF
WEREWOLF.1500a	WULF	PRG	N	1152	1996	WEREWOLF
WEREWOLF.1500b	[WULF]	PRG	N	1152	1995	WEREWOLF
WEREWOLF.1500c	[WULF]	PRG	N	1152	1995	WEREWOLF
WEREWOLF.658	SWEAT_HOME	PRG	N	658	1995	WEREWOLF
WEREWOLF.678	SWEAT_HOME_2	PRG	N	678	1995	WEREWOLF
WEREWOLF.684a	CLAWS	PRG	N	684 - 700	1995	WEREWOLF
WEREWOLF.684b	FANGS	PRG	N	684 - 700	1995	WEREWOLF
WEREWOLF.685a	FANGS	PRG	N	685 - 701	1995	WEREWOLF
WEREWOLF.685b	FANGS	PRG	N	685 - 701	1995	WEREWOLF
WIN32/HLLP.DeTroie.A	WIN32/CHEVAL.TCV	W32-PRG			1998	JCZIC
WM.ALLIANCE.C		WM-DOC			1997	MISTER MAD
WM.ALLIANCE.D		WM-DOC			1997	MISTER MAD
WM.APPDER.A	FUNYOUR, NTTHNTA	WM-DOC	N		1996	
WM.APPDER.R		WM-DOC	D		1998	
WM.CONCEPT.B:FR		WM-DOC	N		1996	
WM.ELOHIM.A:FR		WM-DOC			1998	
WM.INEXIST.A		WM-DOC			1997	
WM.KILLLUF.B		WM-DOC			1997	
WM.NEWYEAR.A		WM-DOC			1997	
WM.NOP.H:FR		WM-DOC			1997	
WM.NUCLEAR.B		WM-DOC	D		1996	
WM.STALL.A		WM-DOC	D		1998	
WM.WAZZU.BE		WM-DOC	N		1997	

APPENDIX 3 (CONTINUED)

VIRUS NAME	ALIAS	TYPE	!!!	SIZE	YEAR	PSEUDO
WM.WAZZU.DG		WM-DOC			1997	SLAM GROUP
WM.WAZZU.DH		WM-DOC			1997	LAVOISIER SCHOOL
WM.WAZZU.DO		WM-DOC	N		1997	Sergiant Thery
WM.WAZZU.DV		WM-DOC	N		1998	
WM.WAZZU.DW		WM-DOC			1998	
WM.WAZZU.DX		WM-DOC			1998	
WM.WAZZU.EY		WM-DOC			1998	
WM.WAZZU.FJ		WM-DOC			1998	
WM.WAZZU.FF		WM-DOC			1998	
WM.WAZZU.FP:FR		WM-DOC			1998	
XF.PAIX.A		XF-XLS			1998	
XF.PAIX.B		XF-XLS			1998	
XM.LAROUX.AD		XM-XLS	N		1997	
XTC.2153		PRG	D	2153	1995	
ZARMA		PRG	N	2322	1994	TURBO POWER

TYPE	BIV-M	Multipartite virus
	BOOT	Boot sector infector (BOOT)
	MBR	Boot sector infector (MBR)
	PRG	File infector (appending)
	PRG_R	File infector (overwriting)
	W32-PRG	File infector (PE – WIN32)
	W95-PRG	File infector (PE – WIN95)
	WM-DOC	Macro-virus (Word)
	XF-XLS	Macro-virus (Excel formulae)
	XM-XLS	Macro-virus (Excel)
!!!	N	Not dangerous
	D	Deliberately dangerous (destructive payload)
	X	Dangerous (bugged)
YEAR		Creating year

References

ACCO A. & ZUCCHELLI E. (1989). LA PESTE INFORMATIQUE *[The Computer Plague]*. Edition Plume. (ISBN:2-9080-3401-8 & 2-7021-1842-9).

BLANCHARD P. (April 1995). PIRATES DE L'INFORMATIQUE – ENQUETE SUR LES HACKERS FRANÇAIS *[Computer Pirates – Survey on French Hackers]*. Edition Addison Wesley (ISBN:2-87908-109-2).

BONTCHEV V. (September 1991). THE BULGARIAN AND SOVIET VIRUS FACTORIES. From the proceedings of the first annual VIRUS BULLETIN Conference.

BONTCHEV V. (April 1998). NO PEACE ON THE EXCEL FRONT. VIRUS BULLETIN.

CLOUGH B. & MUNGO P. (1993). DELINQUANCE ASSISTEE PAR ORDINATEUR – LA SAGA DES "HACKERS", NOUVEAUX FLIBUSTIERS "HIGH TECH"! *[Delinquency Assisted by Computer – The Story of Hackers, new high-tech filibusters]*. Edition DUNOD Tech (ISBN:2-1000-2013-7).

FUHS H. (January 28th, 1997). ENCRYPTION GENERATORS USED IN COMPUTER VIRUSES. EICAR News 3:1.

GORDON S. (1994). THE GENERIC VIRUS WRITER. From the proceedings of the annual VIRUS BULLETIN Conference. Jersey.

GORDON S. (1995) TECHNOLOGICALLY ENABLED CRIME -SHIFTING PARADIGMS FOR THE YEAR 2000. Computers and Security. Elsevier Science Publications.

GORDON S. (1996). WHO WRITES THIS STUFF. ANTIVIRUS ONLINE. IBM. Ed. Joseph Wells.

GORDON S. (1996) THE GENERIC VIRUS WRITER II. From the proceedings of the annual VIRUS BULLETIN Conference. Brighton, UK.

GUISNEL J. (June 1997). GUERRES DANS LE CYBERESPACE - SERVICES SECRETS ET INTERNET *[Cyberspace Wars – Secret Services and Internet]*. Edition La Découverte (ISBN:2-7071-2716-7).

HOFF J.C. (1991). LES VIRUS – METHODES ET TECHNIQUES DE SECURITE *[Viruses – Methods and Security Techniques]*. Edition DUNOD Informatique (ISBN:2-1000-0010-1).

HOFF J. C. (May et June 1996). LES VIRUS EN FRANCE : STATISTIQUES 1995 *[Viruses in France – 1995 statistiques]*. CONFIDENTIEL SECURITE.

HOFF J. C. & PAGET F. (April 1995). LES VIRUS EN FRANCE *[Viruses in France]*. CONFIDENTIEL SECURITE.

HOFF J. C. (May 1994). VIRUS : ETAT DES LIEUX *[Viruses : Assessment]*. CONFIDENTIEL SECURITE.

HOFF J.C. (April 1996). LES VIRUS, APPROCHE QUANTITATIVE ET QUALITATIVE *[Viruses, Quantitative and qualitative Approach]*. SECURITE INFORMATIQUE.

KAMINSKY D. (October 1998). AUTEURS DE VIRUS, ENTREPRISES, EDITEURS D'ANTIVIRUS : LES LIAISONS DANGEREUSES *[Virus Authors, Enterprises, Anti-Virus Editors: Dangerous Affair]*. Paris: CLUSIF.

KARPINSKI D. (October 1994). ANTIEXE.A – MISSING THE TARGET?. VIRUS BULLETIN.

LOINTIER P. with BAKALOVA A. & BONTCHEV V. & HABOV V. (1993). A LA POURSUITE DE DARK AVENGER – L'AFFAIRE DES VIRUS AU GOUT BULGARE *[Chasing Dark Avenger – Viruses in Bulgaria]*. Edition DUNOD Tech. (ISBN: 2-1000-1912-0).

LOVINFOSSE J.P. (1991). LE PIRATAGE INFORMATIQUE *[Computer Piracy]*. Edition Marabout (ISBN:2-501-01542-8).

MUTTIK I. (February 1997). THE WEREWOLF FAMILY: WHEN WOLVES ARE CUBS. VIRUS BULLETIN.

PAGET F. (November 26th, 1997). LES VIRUS, ETAT DES LIEUX *[Viruses, Assessment]*. From the proceedings of the annual PACT Security Forum. Paris, CNIT.

PAGET F. (August 1997). THE FRENCH CONNECTION. VIRUS BULLETIN.

PAGET F. (June 9th, 1995). THE VIRUS SITUATION. From the proceedings of the annual SECURICOM Conference. Paris, La Défense.

RECIF. (October 1993). LES VIRUS EN FRANCE (1) ANNEE 1992 *[Viruses in France, Year 1992]*. STRATEGIE SECURITE.

ROSE P. (1992). LA CRIMINALITE INFORMATIQUE A L'HORIZON 2005 – ANALYSE PROSPECTIVE *[Computer Criminality up to the Year 2005 – Prospective Analysis]*. Editions L'Harmattan & IHESI. (ISBN:2-7384-1498-2).

SMITH G. (1996). VIRUS CREATION LABS EXCERPT. CRYPT NEWSLETTER.

VIRUS BULLETIN (September 1992). TECHNICAL NOTES - VIRUS CONSTRUCTION TOOLS. VIRUS BULLETIN.

WELLS J. THE WILDLIST - PC VIRUSES IN THE WILD. Monthly report. http://www.wildlist.org.

WHALLEY I. (April 1995). JUMPER: JUMPING THE GUN. VIRUS BULLETIN.

Definitions of some terms and glossary

40Hex: Underground viral magazine from Phalcon-Skism Group (USA). Publications from 1991 to 1995.

Alias: a different name by which a virus is known.

Anti-debug techniques: code generally implemented at the beginning of the virus in order to make it harder for anti-virus researchers to debug the virus.

Back Orifice: executable released by a hacker group called Cult of the Dead Cow in July 1998. According to its creators, Back Orifice is «self-contained, self-installing utility, which allows the user to control and monitor computers running the Windows operating system over a Network».

Boot sector infector: a virus that infects the system area on a floppy disk and/or on a computer system (boot sector or master boot record).

Bug: an unintentional fault in a program.

Cell formula: cell originally encountered in Excel 4.0 macro sheets allowing the user to create automated routines with the macro language. With Excel 5.0, a new VBA macro language was introduced but for compatibility reasons both languages cohabit in the actual Excel versions.

Cylinder: all the tracks on a disk that are the same distance from the center.

Drive head: one of the read/write coils in a disk drive

Encrypted virus: an encrypted virus consists of two parts, a decryption program and the encrypted body of the virus. Virus writers created this technique to prevent detection via string-based scanning more difficult.

File infector: a virus that infects executable files.

Head: one of the read/write coils in a disk drive.

In-the-wild: a term used by virus researchers to describe any virus that has infected a computer and that has been reported outside a virus research site.

Macro: a program used usually for automating some processes inside an application. Visual Basic for Applications (VBA) and WordBasic (WB) are the languages used by Microsoft.

Macro-virus: a piece of self-replicating code written in an application’s macro language and usually associated with a data file.

Memory-resident virus: a virus that remains in the PC’s memory after it has been executed.

Multipartite virus: A virus which uses a combination of techniques to spread, for example, infecting both files and boot sector.

Overwriting virus: A virus which overwrites each file it infects.

Payload: what a virus does when it triggers.

PE file infector: a virus that infects the new executable files supported by Win32, Windows NT and Win95/98. This file format is called Portable Executable (PE) file format.

Polymorphic virus: a virus that alters the next incarnation with a slightly different algorithm. With this scheme, it is harder to fixed patterns perhaps without decrypting the code.

Sector: part of a track, usually 512 bytes long.

Stealth virus: a virus that tries to avoid detection in order to conceal its presence when it is memory-resident.

Track: All the sectors around the disk on a single head and at a same distance from the center. Referred to also as a cylinder.

Trigger: the condition that causes a virus to deliver its payload (for example, date, number of re-boots, etc.).

VBA module: a collection of macros written in the Visual Basic for Applications (VBA) language.

VDAT encyclopedia: underground electronic document, compilation of files about viruses and anti-viruses. It is considered to be the "Who and What" of the virus scene by the virus writer community.

Virus variants: a variation of a virus, usually caused by a minor change to the code of an existing virus.

VMACRO: INTERNET discussion group dedicated against macro viruses and consisting of many of the anti-virus researchers around the world.

Abbreviations

AVERT: Anti-Virus Emergency Response Team
BBS: Bulletin Board System.
BCRCI: Brigade Centrale de Répression de la Criminalité Informatique
CAP: Carlos Andrés Pérez, political figure in Venezuela
CARO: Computer Anti-Virus Researchers Organization.
CLUSIF: CLub de la Sécurité Informatique Française
DST: Direction de la Surveillance du Territoire
EICAR: European Institute for Computer Anti-Virus Research
MDMA: Many Delinquent Modern Anarchists
NPAD: National Panics Anxiety Disorder
NAI: Network Associates
PE: Portable Executable
RECIF: Recherche et Etude sur la Criminalité Informatique Française
SEFTI: Service d'Enquête sur les Fraudes aux Technologies de l'Information
VB: Virus Bulletin
VCS: Virus Construction Set

Useful Addresses

BCRCI: Brigade Centrale de Répression de la Criminalité Informatique. 101, rue des 3 Fontanots. 92000 – Nanterre. France
Tel: +33 (0)1 40 97 87 72. Fax: +33 (0)1 47 21 00 42

CLUSIF: CLub de la Sécurité Informatique Française. Tour Aurore. 18, place des Reflets. 92975 – Paris La Défense Cedex. France
Tel: +33 (0)1 47 78 63 33. Fax: +33 (0)1 47 78 63 13

CONFIDENTIEL SECURITE: 83 ter rue Carnot, 60200 – Compiègne.
Tel: +33 (0)3 44 86 33 66. Fax: +33 (0)3 44 86 25 26

DST: Direction de la Surveillance du Territoire. Ministère de l'Intérieur. 7, rue Nélaton. BP 514. 72727 – Paris Cedex 15. France
Tel: +33 (0)1 40 57 55 34. Fax: +33 (0)1 40 57 54 88

EICAR: European Institute for Computer Anti-Virus Research. Hochstallerweg. 28. D-86316. Friedberg. France
Fax: +49 (0)821 606786

NETCOST & SECURITY: 55, quai de Bourbon, 75004 – Paris.
Tel: +33 (0)1 46 33 38 39. Fax: +33 (0)1 46 33 10 28

RECIF: Recherche et Etude sur la Criminalité Informatique Française. BP109. 95130 - Le Plessis Bouchard. France

SEFTI: Service d'Enquête sur les Fraudes aux Technologies de l'Information. 163, avenue d'Italie. 75013 – Paris. France
Tel: +33 (0)1 40 79 67 50. Fax: +33 (0)1 40 79 77 21

VB: Virus Bulletin Ltd. The Pentagon. Abingdon Science Park. Abingdon. Oxfordshire. OX14 3YP. England.
Tel: +44 (0)1235 555139. Fax: +44 (0)1235 531889