Virus Longevity—Virus Lifecycle

Larry Bridwell
Content Security Programs Manager
ICSA Labs, a division of TruSecure Corp
and
Jaime Lyndon A. Yaneza
Global Anti-Virus Research Group
TrendLabs, Trend Micro Inc.

The big questions:

- How many viruses are there?
- How many viruses are there in circulation?
- How long do viruses survive?
- Why do some viruses last longer than others?
- What can limit the longevity of a computer virus, or a whole type of computer viruses?

How to answer our questions?

- The WildList Organization is one of the better sources for tracking virus data.
- ICSA Labs Annual Virus Surveys

WildList Organization

- Established by Joe Wells in 1993
- First official published list November 1993
- Since then, the WildList has grown into the world's foremost authority on which viruses users should really be concerned with.
- Currently used as a basis for testing antivirus software by proficient and competent testing authorities
- The WildList remains available free to computer users worldwide.

ICSA Labs' Surveys

- ICSA Labs has produced Virus Prevalence Surveys since 1994
- ICSA Labs' Computer Virus Prevalence Survey is an annual survey of computer viruses and worms.
- The survey reports information about
  - incidents experienced
  - financial impact
  - disaster characteristics
  - anti-virus product use
  - forecasts trends

Back to our questions…

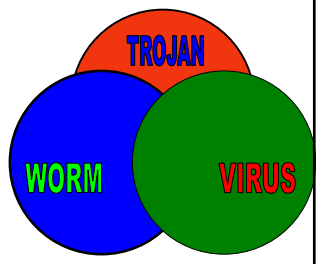
- How many viruses are there?
- How many viruses are there in circulation?
- How long do viruses survive?
- Why do some viruses last longer than others?
- What can limit the longevity of a computer virus, or a whole type of computer viruses?

What constitutes survival?

- For this presentation, a virus will be said to survive, IF…
  - A virus stays on the WildList
  - It is reported at least quarterly
  - Is found in the "top ten" on
    - ICSA Labs surveys
    - Public sources

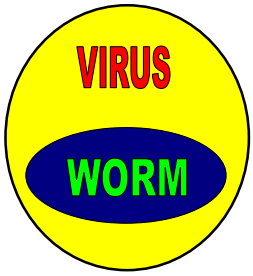
History of viruses contiguous?

Throughout the history of computer malware, there has always been no clear definition consensus of taxonomy.

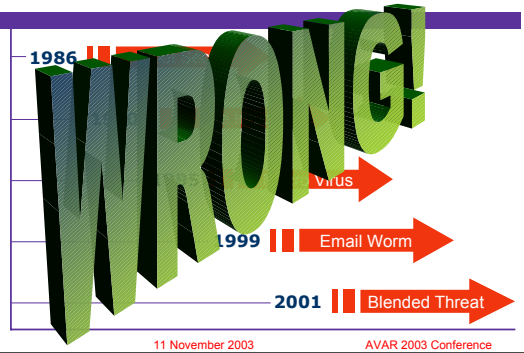


For this presentation a virus is…

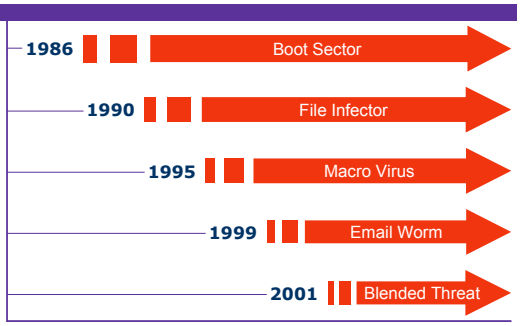
A virus is self-replicating code and a worm is a type of virus



Virus Eras



Virus eras



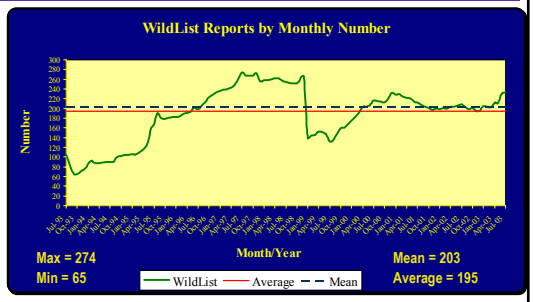
HOW MANY VIRUSES?

- There has always been a distinction between viruses *In the Wild* and those known viruses in *zoos.*
- *In the Wild* refers to those that have been reported to actively infect computers of end users.
- *Zoo* Viruses refer the many viruses known to researchers that have never been a threat to end users.

How many viruses are a threat?

- ~80,000 - viruses ever known
- ~2,000 - viruses ever In the Wild!
- ~205 - Mean # ItW!
- ~195 - Average # ItW!

How many viruses are a threat?



Each virus has a lifecycle!

Elements of a virus lifecycle

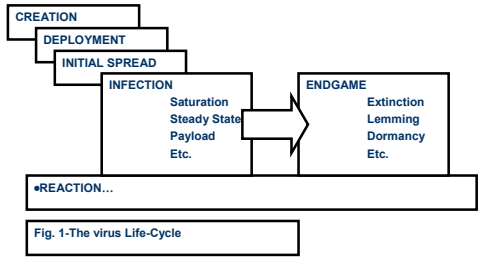
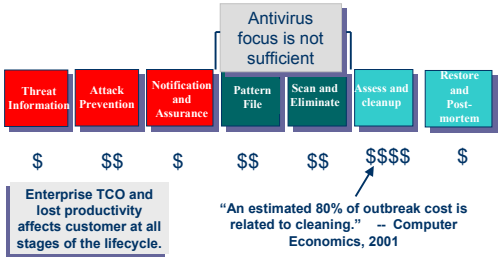


Fig. 1-The virus Life-Cycle

A view of the virus lifecycle



Virus Outbreak Lifecycle = Customer Experience

What makes some viruses survive longer than others?

What makes some viruses….?

- Are some viruses better written than other viruses?
- Do some virus *types* survive better?
- Does the media reaction (and the subsequent user and administrator reaction) limit the lives of some viruses?
- Is there some kind of event that can limit a virus?
- Is there some macro event that can limit the life of a given virus type?

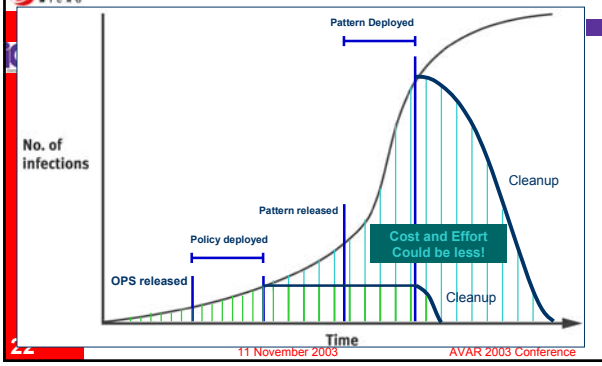
Extinct Viruses?

- The computing environment changes, but it is slow to change. A virus or virus type "obsolete" today is not necessarily "Extinct" and may well show up regionally.
- EG.—boot sector viruses were obsolete in 1995, but still were written until very recently and are still found ItW today!

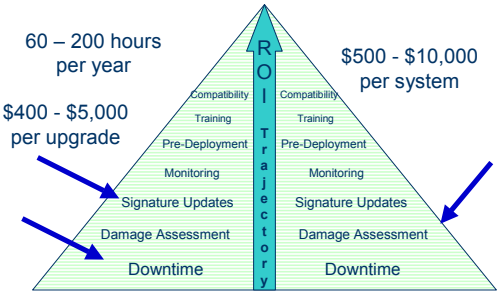
Things that can cause extinction

- If the virus itself is too destructive, it is considered to wipe itself out of existence! This is called a *lemming!*
- If a virus relies on a given webpage or server for it's replication process, it will be made extinct.
- A change in the OS or hardware standard (or application) can either begin or end a new virus or an entire type
- Some viruses have an expiration date!
- If protection against a given type of virus gets very effective, it makes that type obsolete!

Lifecycle awareness may help



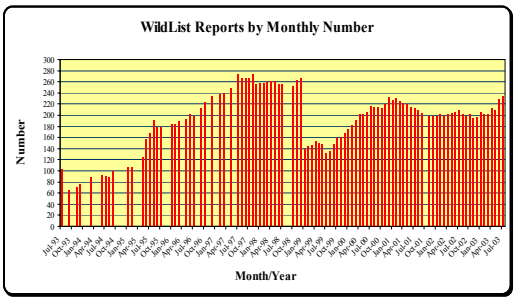
Business Concerns



Source: Gartner Group, August 2002

The DATA

Viruses Reported



93-98 Top Viruses

Rank	Virus
1	Cascade.1701.A
2	Cascade.1704.A
3	Changsha.3072
4	Chinese_Fish
5	Dark_Avenger.1800.A
6	Dir_II.A
7	Flip.mp.2153.A
8	Flip.mp.2343.A
9	Form.A
10	Helloween.1376.A
11	Jerusalem.1808.Standard
12	Jerusalem.Zero_Time.Australia
13	Joshi.A
14	Keypress.1232.A
15	November_17th.855.A
16	Parity_Boot.B
17	Stoned.Azusa
18	Stoned.June_4th
19	Stoned.Manitoba
20	Stoned.Michelangelo
21	Stoned.No_INT
22	Tequila
23	Tremor.A
24	Vienna.648.Reboot.A
25	V-Sign
26	Yankee Doodle.XPEH

'99-'03 Top Viruses

Rank	Virus
1	AntiCMOS.A
2	AntiEXE.A
3	Empire.Monkey.B
4	Form.A
5	One_Half.mp.3544.A
6	W95/CIH.1003
7	W95/CIH.1019.A
8	W97M/Class.D
9	W97M/ColdApe.A
10	W97M/Groov.A
11	WM/CAP.A
12	WM/Concept.A
13	WM/Copycap.A
14	WM/Npad.A
15	WM/Wazzu.A
16	X97M/Laroux.A
17	X97M/Laroux.DX
18	X97M/Laroux.E
19	XM/Laroux.A

Top Reported Viruses '93-'03

Rank	Virus
1	Form.A
2	AntiEXE.A
3	AntiCMOS.A
4	Parity_Boot.B
5	Ripper
6	Stoned.Michelangelo
7	Junkie.mp.1027.A
8	WM/Concept.A
9	Stoned.No_INT
10	WM/Wazzu.A

Top Reported Viruses ICSA Surveys

1997	1998	1999	2000	2001	2002	2003(?)
WM Concept	WM/Concept	Melissa	W97M/Melissa	Sircam	Klez	BugBear
Macro-Unspecified	WM/Wazzu	Class	VBScript -Unspecifiedd	LoveLetter	BugBearf	Dumaru
Form.A	WM/CAP	Laroux	Worm - unspecified	Homepage	BadTrans	Klez
Anti-EXE	XM/Laroux	Wazzu	Macro-unspecified	Funlove	Yaha	Magistr
WM Wazzu	Stealth B	Ethan	JS/Kak	Anna Kournikova	Sircam	Mimail
Monkey B	NYB	CAP	W32/PrettyPark	Macro-Unspecified	Funlove	Nimda
NYB	Form.A	Ska	W97M/Marker	Magistr	LoveLetter	Sober
WM Npad	AntiCMOS	CIH	VBS/Freelinks	Hybris	Elkern	Sobig
Stealth B	WM/Npad	Concept	X97M/Laroux	Melissa	Magistr	Swen
Junkie	AntiEXE	Macro-Unspecified	W32/Ska	CodeRed	Nimda	Yaha

So...

- How many viruses are there?
  - A lot
- How many viruses are there in circulation?
  - Only a relatively small percentage of those
- How long do viruses survive?
  - Life span can be long, but effectiveness is growing shorter
- Why do some viruses last longer than others?
- What factors limit the longevity and effectiveness of a computer virus?
  - Virus delivery & infection vectors
  - Human factors
    - Social engineering, lack of: diligence, updating, "complete" recovery
  - Technology changes – new protocols, platforms, file systems, etc.

Questions

Larry Bridwell
ICSA Labs
lbridwell@icsalabs.com

Jamz Yaneza
Trend Micro, Inc.
Jamz_Yaneza@trendmicro.com