

WORMS 2.0

Evolution — From SyFy to "You Die"


Nelson Brito

nbrito@br.ibm.com



Those who do not remember the
past are condemned to repeat it.

GEORGE SANTAYANA



WORMS 2.0

Introduction





A computer WORM is a self-contained program (or set of programs), that is able to spread functional copies of itself or its segments to other computer systems (usually via network connections).

VIRUS-L/COMP.VIRUS

Frequently Asked Questions (FAQ) v2.00



WORMS 2.0

From SyFy to "You Die"





Yes, sir! I'm quite aware that an worm of that type is theoretically impossible! But the fact stands, he's done it, and now it's so goddamn comprehensive that it can't be killed. Not short of demolishing the net!

JOHN BRUNNER

The Shockwave Riders



The "worm" programs were an experiment in the development of distributed computations: programs that span machine boundaries and also replicate themselves in idle machines.

JOHN F. SHOCH & JON A. HUPP

The "Worm" Programs — Early Experience with a Distributed Computation



Hospitals and doctors' surgeries in parts of England were forced to turn away patients and cancel appointments [...] People in affected areas were being advised to seek medical care only in emergencies.




CHRIS GRAHAM
The Telegraph News

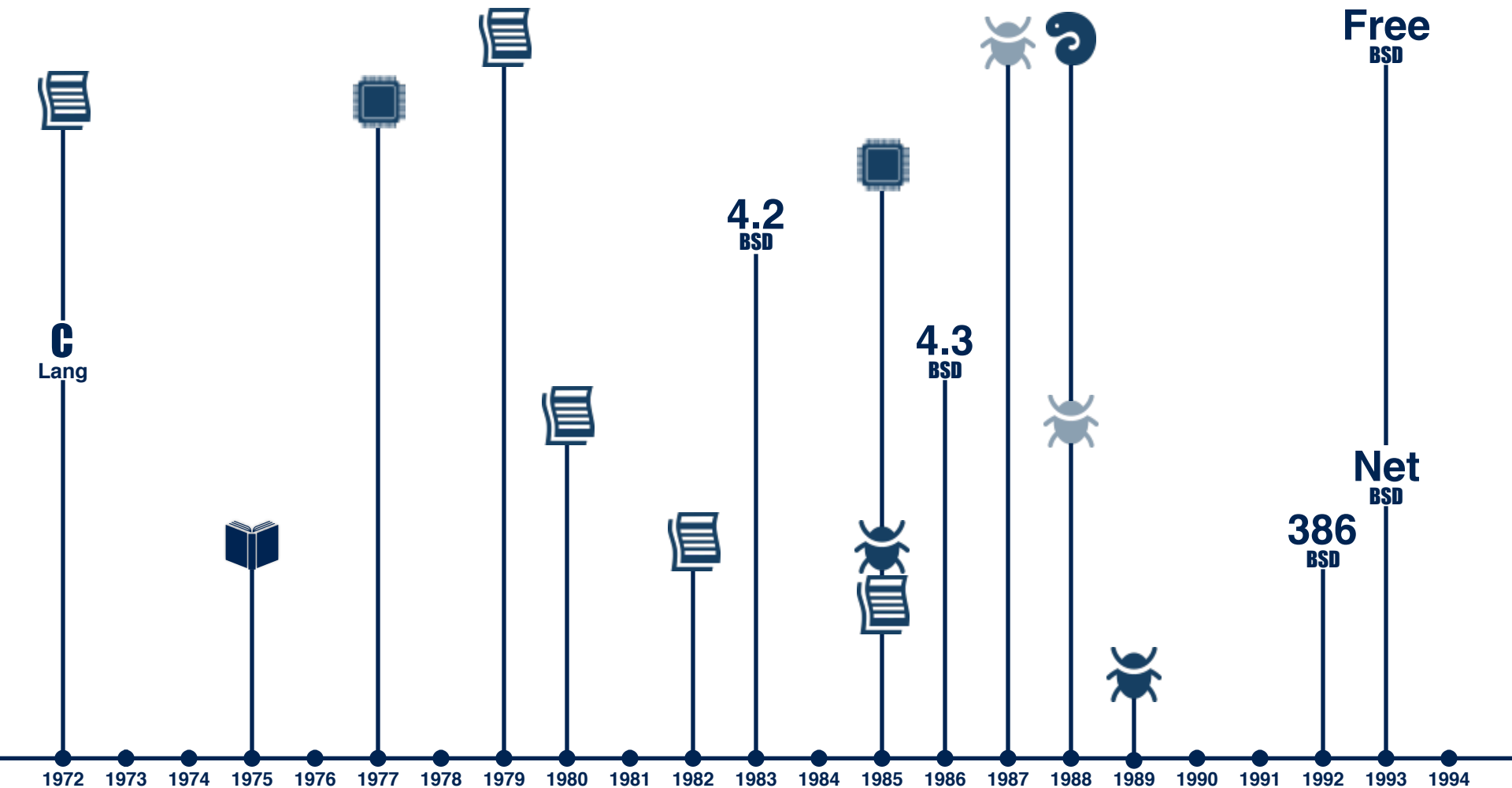


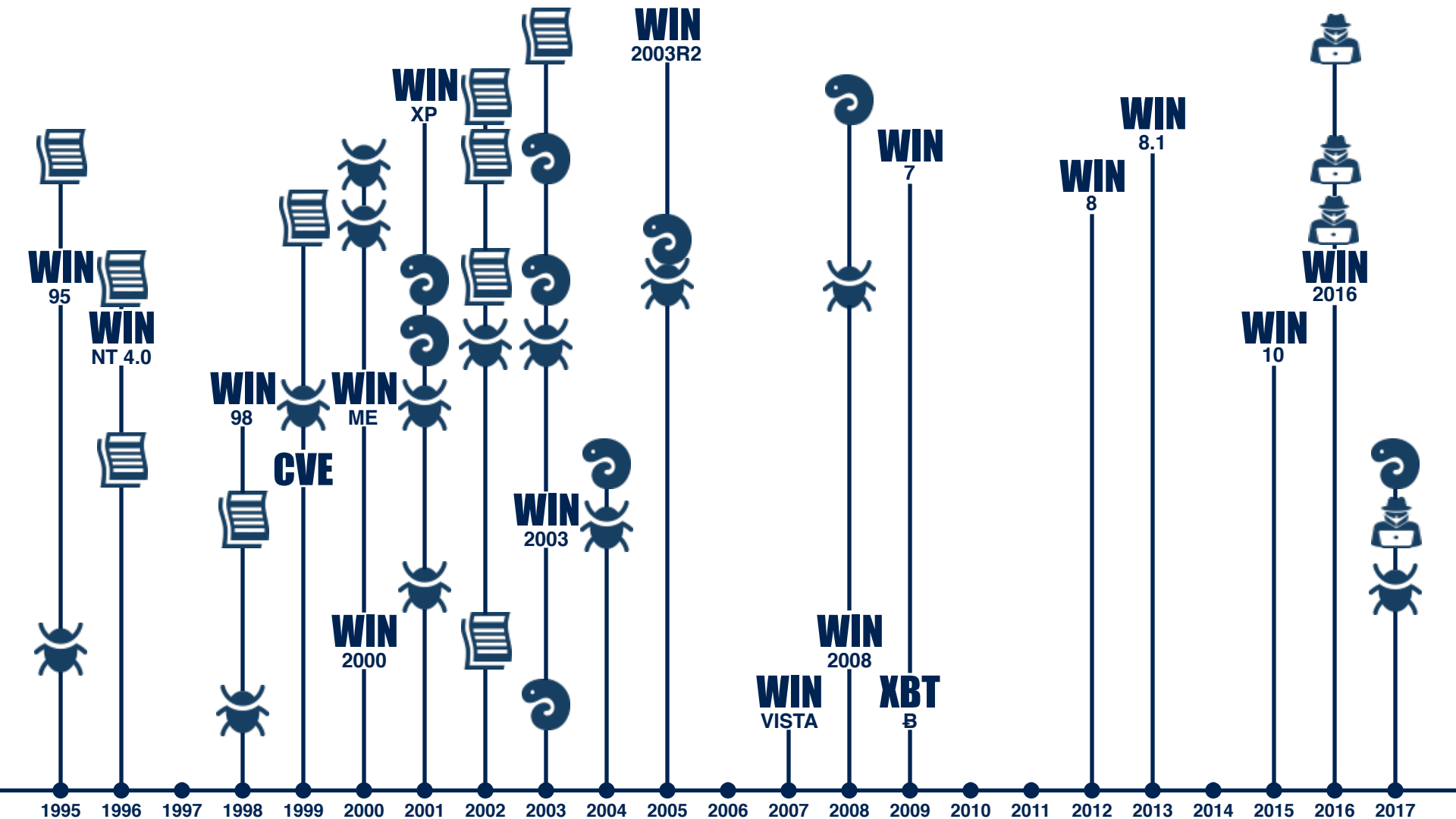
WORMS 2.0

The Rise of Worms



Document	Book	Hardware	Vulnerability	Worm	Hacker(s)
					







WORMS 2.0






Conclusions (Q&A)





THANK YOU!

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2017. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.

IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.