

New cyber risk: premises for an insurance coverage

Maria Elena Addressi¹ - Alessandro Annibali² - Carla Barracchini³

In literature, we have not found insurance policies created to evaluate and to pay the damages that follow an attack of computer piracy. Encouraged by the widespread attacks via the Internet and after having considered the extent of such a problem, a mass phenomenon so far, we would like to write our reflections on the cyber risks via web which, beyond any material damages, can also cause damages to the image and privacy violation. On the analogy of the coverage regarding health insurance, three levels of damage can be identified with regard to the functionality of the computer. In this paper, we have hypothesised a structure of the probabilistic model in order to describe the damages after the networking. Therefore, we have proposed a possible solution to the problem through insurance policies. The aim of this working paper is not to propose a technological solution, but to hypothesise the actuarial premises for the coverage about net damages

Key-words

Computer virus, worm, trojan, cyber risk, insurance.

Jel classification: G22, L86.

1. Introduction

The use of the Internet favours the transmission of information and programs. Some of these programmes (viruses) are lines of code that modify the software and/or the information contained in a terminal.⁴ The virus is a form of violence, deceitful and invasive, for which, at the moment, no reliable tools of prevention and defense exist. Following the use of the net, these viruses multiply and become more and more advanced (*Trojan*⁵, *Worm*⁶).

¹ Lumsa – Libera Università Maria SS Assunta, Rome m.addressi@lumsa.it

² Eurokleis Srl –Research Innovation Finance, Rome alexannibali@openaccess.it

³ Dept. of Systems and Institutions for Economics, University of L'Aquila carlab@ec.univaq.it

⁴ We refer hereinafter to a terminal as any device that can be connected to the web (via the Internet and/or Intranet)

⁵ The Trojan viruses are composed of two files: Client and Server. The file Server is an executable that, in an invisible way, settles in the computer allowing those one who possess an equivalent Client type file to enter the system. The most known Trojan viruses are BackOrifice, NetBus and BACKDOOR-G [wikipedia.org].

⁶ The Worm viruses are programmes that act on the operating system and spread, generally, through emails [wikipedia.org].

The aim of this working paper is not to propose⁷ a technological solution, but to hypothesise the actuarial premises for the coverage about net damages.

By risk of cyber piracy (hackers) we mean the possibility to receive a virus that limits the operation of the terminal⁸.

In this paper, a via-web connected computer is the object of the coverage. Starting from multistate models for health insurance [Pitacco (1995), Pitacco-Olivieri (1997)], we have hypothesised two typologies of computer policies:

- ADC (Activities of Daily Cyber)
- GCU (Good Cyber Use)

2. State of the art

The virus is a programme that generates other programmes, being this process an automatic procedure (Base minima di sicurezza (2002)).

The first virus (Figure 1) has been created by the mathematician von Neumann (1948).

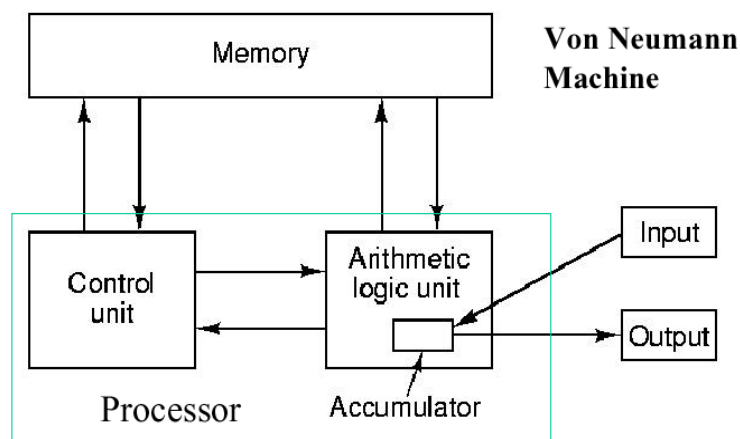


Figure 1

Solomon and Slade⁹ have studied and classified the main viruses since 1981.¹⁰

⁷ For instance, the software-distributing houses (Symantec, McAfee, Pccillin, etc) have put on the market antivirus programmes which should neutralise the action of the viruses (Worm, Trojan).

⁸ The malfunctioning of the terminal can be caused by an interruption of connection, a loss of data, a transmission of information to a third not-authorized party, a missed access to applications, a limited use of the memory, a reduction of speed – regardless the risk time, both in economic and programmable terms.

⁹ <http://www.cknow.com/vtutor/vthistory.htm>

¹⁰ 1981: the first virus in the wild: Elk Cloner; 1983: The First Documented Experimental Virus; 1986: Brain, PC-Write Trojan, & Virdem; 1987: File Infectors, Lehigh, & Christmas Worm; 1988: MacMag, Scores, & Internet Worm; 1989: AIDS Trojan; 1990: VX BBS &

Cohen (1987) has examined the algorithm describing the propagation of a virus through a test on the virus known as Elk Cloner (1981).

Other Authors have proposed stochastic models of propagation for specific typologies of viruses (*Worm, Trojan* and so on).

*Symantec Internet Security Report*¹¹ has shown that Hackers use more and more such worms in order to exploit known vulnerabilities and, therefore, to create accesses to a huge number of systems.

The 64% of new attacks have concerned vulnerability of recent softwares; the reason is that antivirus companies have not had enough time to study the holes of the antivirus itself and the hackers have had much time to attack. It is evident that old softwares are safer than young ones.

The same research has shown that Hackers use more and more the worms in order to exploit known vulnerabilities and, therefore, to create accesses in a huge number of systems.

In the *Official Journal* of March 22, 2002 a document was published under the title "Base minima di sicurezza": it deals with the guidelines for the individualisation of the protection measures for the Public Administration

The same document shows that most programmes for terminal safety are not able to neutralize all the possible threats. In this paper, we aim at proposing an actuarial model for the coverage of the consequential computer risks from the use of the net¹².

3. The cyber risk

It is necessary to catalogue the cyber risks with the purpose of individualising the component at the basis of the GCU and ADC coverage. An insurance policy pertains to a risk that refers both to an economic element (a covered interest) and to a probabilistic element (harmful events and their probabilities).

In order to classify the level of gravity and, therefore, of riskness of the viruses, Symantec proposes:

- a) the degree of spread;
- b) the seriousness of the damage;
- c) the speed of virus propagation.

Little Black Book (AT&T Attack); 1991: Tequila; 1992: Michelangelo, DAME, & VCL; 1995: Year of the Hacker; 1995: Concept (The first macro virus was developed to attack Word); 1996: Boza, Laroux, & Staog; 1998: Strange Brew & Back Orifice; 1999: Melissa, Corner, Tristate, & Bubbleboy; 2000: DDoS, Love Letter, Timofonica, Liberty (Palm), Streams, & Pirus; 2001: Gnuman, Winux Windows/Linux Virus, LogoLogic-A Worm, Apls/Simpsons Worm, PeachyPDF-A, Nimda; 2002: LFM-926, Donut, Sharp-A, SQLSpider, Benjamin, Perrun, Scalper; 2003: Slammer, Sobig, Lovgate, Fizzer, Blaster/Welchia/Mimail; 2004: Trojan.Xombe, Randex, Bizex, Witty, MP3Concept, Sasser, Mac OS X, W64.Rugrat.3344, Symb/Cabir-A, JS/Scob-A, WCE/Duts-A.

¹¹ <http://www.symantec.com>

¹² Assicurazioni Generali has proposed "Polizza reti" and "Polizza di tutti i rischi informatici" (www.generali.it) but, to our knowledge, the actuarial models of reference have not been made known.

It is not interesting to classify the viruses on the basis of the technical characteristics, but on the basis of the damages they can provoke. On the analogy of the coverage regarding health insurance, three levels of damage can be identified with regard to the functionality¹³ of the computer:

Computer Insurance	Health Insurance
No damage (<i>nd</i>)	Self-sufficient
Repairable damage (<i>rd</i>)	Temporary invalidity
Partially repairable damage (<i>prd</i>)	Permanent invalidity
not repairable damage (<i>nrd</i>)	Death

Table 1

We indicate with $(1, \dots, m)$ the m -vector of computer activities (operating system, email management, operation of the programmes, management of the database), and with $(\omega_1, \dots, \omega_m)$ ($\omega_i \in \mathbf{N}$) the vector of the weights¹⁴ attributed to such activities; we define with

$$\alpha = \left\{ \begin{array}{l} \\ \\ \\ \end{array} \right.$$