Chapter 5

Malware:
Can Virus Writers be Psychologically Profiled?

ABSTRACT

Most computer users are likely to have some exposure to malware (malicious software), in the form of spyware, computer viruses, worms or Trojans. This chapter aims to determine if malware developers, and in particular virus writers, can be psychologically profiled. Initially, the chapter will clarify the distinctions between different types of malware, and provide a brief history of some of the most famous malware programs which have been developed. It is important to remember that malware producers and hackers are not necessarily the same individuals, although there is no doubt that at least some individuals engage in both behaviours and the terms are sometimes used interchangeably in the media. A key researcher in the psychology of virus writers, Sarah Gordon, distinguishes between hackers and virus writers "In general, hackers frown upon virus writers. After all, hacking requires system knowledge and skill and is somewhat "sexy" in today's counterculture, while virus writing is still looked down upon, mostly for its indiscriminate damage and lack of required skill" (PBS Frontline, n.d., no pagination). The psychology of hackers and the skills required to engage in hacking activities have previously been described in Chapter 4, and while there is some overlap, it is certain that there are differences between the methods, motives and skills of the two groups.

Malware is prolific, and the known prevalence rates for infection, as well as the quantity of known malware programs, will be identified. A brief overview of how malware applications are developed and distributed will be considered, especially in light of the use of social psychology in encouraging individuals to download and distribute the programs. However there is a lack of empirical psychological study relating to virus writers, and much of the literature is based on case studies and individual interviews. Nevertheless, some tentative explanations for the motives of virus writers can be put forward, and there is some limited information available regarding the psychological profile and personality characteristics of virus writers.

In particular, similarities with the psychology of vandalism will be explored, in order to determine if similar theories might explain both phenomena. The chapter will also explore methods of reducing and preventing damage done by malware, and it will explore the psychological mechanisms that can predict if a computer user is likely to engage in safe online behaviour. Finally consideration will be given to future trends in malware development, such as the increasing threat of malware on portable devices, and suggestions for important future research in the area.

BACKGROUND

An early computer virus type program was known as 'cookie monster'. This relatively benign virus would prevent the user from using the computer by requesting a cookie. If the user typed in the word 'cookie', the message would disappear, only to reappear a while later requesting another treat. The 'cookie monster' virus was an irritation, but more modern viruses can have considerably more serious consequences.

In September 2010, the Stuxnet worm inflicted damage on computers and networks, mostly in Iran. While it was first detected in June 2010, it was in September 2010 that it was revealed that the worm had infected computers at Iran's first nuclear power station (BBC News, 2010a). The Stuxnet worm specifically targets systems used to manage utilities such as water, oil rigs and power plants. It is a highly tailored worm, and is thought to be the first worm designed to target such facilities. Instead of using the Internet to distribute itself it infects Windows via portable memory devices such as USB keys. Because of this it can target systems that are not connected to the Internet for security reasons. Once infected, the worm can reprogram the software which gives instructions to industrial machinery, such as motors and coolers, telling them to turn on or off at given signals. As this worm looks for very specific configurations, and does not actively affect the system unless it finds them, this case has obvious implications for the potential of cyberterrorism (see Chapter 11), although at the time of writing, there is insufficient evidence to determine who wrote the worm or what its intended target was (BBC News, 2010b).

However, Ralph Langner (an industrial computer expert) is quoted by BBC News (2010b) as saying that "With the forensics we now have it is evident and provable that Stuxnet is a directed sabotage attack involving heavy insider knowledge" (no pagination).

Definitions and Categories of Malware

Edgar-Nevill and Stephens (2008) define malware as "any piece of software devised with malicious intent" (p. 91). The term is taken from the phrase 'malicious software' and is used to describe any software program that spreads from one computer to another and that interferes with computer operation. Kramer and Bradfield (2010) indicate that while malware is intuitively considered to be "software that harmfully attacks other software, where to harmfully attack can be observed to mean to cause the actual behaviour to differ from the intended behaviour" (p. 105). However, Kramer and Bradfield claim that this definition is insufficient, as the intended behaviour is infrequently defined, and so a more accurate definition of malware needs to also consider the concept of "software system correctness" (p. 105), and proceed to define this in technical terms. They go on to define other related concepts including 'benware' (benign software) and 'anti-malware' ('antibodies' against malware).

Important terms relating to malware include 'payload' and 'in the wild'. 'In the wild' refers to how widespread the malware is. Malware such as viruses are not always released, and may be developed as a 'proof of concept' which remains

Related Content

Task Offloading in Cloud-Edge Environments: A Deep-Reinforcement-Learning-Based Solution
Suzhen Wang, Yongchen Dengand Zhongbo Hu (2023). *International Journal of Digital Crime and Forensics (pp. 1-23).*
www.irma-international.org/article/task-offloading-in-cloud-edge-environments/332066

Providing Cryptographic Security and Evidentiary Chain-of-Custody with the Advanced Forensic Format, Library, and Tools
Simson L. Garfinkel (2011). *New Technologies for Digital Crime and Forensics: Devices, Applications, and Software (pp. 1-28).*
www.irma-international.org/chapter/providing-cryptographic-security-evidentiary-chain/52841

Golden Eye: An OS-Independent Algorithm for Recovering Files From Hard-Disk Raw Images
Fan Zhang, Wei Chenand Yongqiong Zhu (2022). *International Journal of Digital Crime and Forensics (pp. 1-23).*
www.irma-international.org/article/golden-eye/315793

Fight Against Corruption Through Technology: The Case of Morocco
Hicham Sadok (2023). *Concepts, Cases, and Regulations in Financial Fraud and Corruption (pp. 302-316).*
www.irma-international.org/chapter/fight-against-corruption-through-technology/320029

Digital Image Splicing Detection Based on Markov Features in QDCT and QWT Domain
Ruxin Wang, Wei Lu, Jixian Li, Shijun Xiang, Xianfeng Zhaoand Jinwei Wang (2020). *Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice (pp. 61-79).*
www.irma-international.org/chapter/digital-image-splicing-detection-based-on-markov-features-in-qdct-and-qwt-domain/252679