THE PRIMARY DANGEROUS COMPUTER VIRUSES

Student's Name

Course:

Tutor:

Institutional Affiliation:

Date:

The Primary Dangerous Computer Viruses

In the current times, the highly computer-dependant environment is characterised with increased instances of computer security, for instance, threats elicited by computer viruses. Therefore, this essay will provide a discussion on primary and dangerous computer viruses. The history of computer viruses can be traced back to the early 1980s with Khan (2012) outlining the number of computer viruses created over the last two decades. The historical development of computer viruses ranges from simple activities where hackers sought bragging rights to extreme cybercrimes where organisations and individuals loss vital information and billions of money. In their studies, Joshi and Patil (2013), and Khan (2012) point out numerous types of primary computer viruses, how they are triggered, implication, and their respective examples.

First, resident viruses are notable for their existence in a computer's random access memory (RAM) where they interrupt operations that are executed in the system by corrupting open files and programs. Examples of this virus include the likes of Randex and Mrklunk. Program or file viruses are another set of potential and dangerous computer viruses that is evidenced with infection instances of executables, such as the .exe, .bin, .com, and .sys file systems (Joshi and Patil, 2013; Khan, 2012). Examples of this computer virus include Cascade and Sunday viruses. The computer virus in the category of boot sector viruses affects the booting sectors of a computer's flop, USB, or hard disk drive, which houses the boot system. When the boot system is compromised, the affected computers cannot power on. Some of the examples of this virus include the Polyboot.B, Disk Killer, Stone virus, and the AntiEXE virus.

The other type of virus is identified as the multipartite viruses that are characterised with adverse implications, such as destroying or altering computer programs and stored data.

Examples of this virus that have similar features with the boot sector viruses are Invader, Tequila, and the Flip viruses. In addition to these three types of viruses, other primary groups that pose dangerous implications can be identified as the direct action viruses, overwrite viruses, polymorphic virus, and macro virus among others. These have their own unique features for differentiation by specialists as they design remedies to halt their replication before they are transferred from one computer to another one (Wanjala and Jacob; 2017; Yusuf, Onotehinwa, and Okon, 2017).

Conclusively, this essay has identified several primary computer viruses that can cause potential damage when they get into a user's computer. Examples of these computer viruses, such as resident viruses, multipartite viruses, direct action viruses, overwrite viruses, and boot sector viruses have varying features and tend to attack different components of a computer.

References

Joshi, M.J. and Patil, B.V., 2013. Computer virus: Their problems and major attacks in real life. *International Journal of P2P Network Trends and Technology, 3*(4), pp.205-209.

Khan, I., 2012. An introduction to computer viruses: problems and solutions. *Library Hi Tech News, 29*(7), pp.8-12.

Wanjala, M.Y. and Jacob, N.M., 2017. Review of Viruses and Antivirus patterns. *Global Journal of Computer Science and Technology, 17*(3), pp.1-3.

Yusuf, M.S., Onotehinwa, T.O., and Okon, E.O., 2017. Productivity of business enterprises: effect of computer virus infection on files. *International Journal of Computer Science and Mobile Computing, 6*(2), pp.179-193.