The Viability of the Malaysian Penal Code in Handling Physical Damage Caused by Malware

Rizal Rahman[†], **Mohd Sophian Zakaria**[††]
noryn@ukm.edu.my sophian@agc.gov.my
[†]Malaysian and Comparative Law Centre, Faculty of Law, Universiti Kebangsaan Malaysia
[††] Attorney General Chambers of Malaysia

Summary

There is no assurance that malware could only cause virtual damage to computer programs and data as its potential is endless. However, legal provisions were earlier developed to cater to either a physical damage caused by a physical action or a virtual damage caused by a virtual action. When crossovers occur, it becomes quite uncertain as to how viable the current laws are in handling this matter. The author seeks to address the issue from the perspective of the laws of Malaysia.

Key words:
malware; damage; Penal Code; Malaysia;

1. Introduction

When the Trojans saw the wooden horse, they rejoiced in what they considered to be the Gods' blessing upon them and an omen against the Greeks. They ignored their priest Laocoön's warning: "Timeo Danaos et dona ferentes" (I fear Greeks, even those bearing gifts) [1], and did not realise that what they saw was not what it seemed to be. Thousands of years later, the metaphor of the wooden horse reappeared in the form of computer hardware in the famous United States case of the "Manchurian chips". where fearing that integrated circuits imported from other countries for use in the military infrastructure might contain malicious components that could be used by others to compromise national security, the Department of Defense of the United States, via the Defense Advanced Research Projects Agency (DARPA), launched the "Trust in Integrated Circuits program" to monitor the circuits [2] [3]. Unlike the Trojans, the Americans acted to the contrary. The pre-emptive action by the United States was considered a wise step, considering that any interference to the military infrastructure by foreign hackers acting remotely could cause damage to life and property in the American soil [4].

There is a direct analogy between the Trojan tragedy and the digital invasion of *malware*. Some of the variants break into a user" s computer system straight away like intruders who do not understand the value of the word "permission", while others creep in like invaders temporarily wearing well behaved attitudes, pleading to gain the user" s trust and sympathy. However, when the permission is granted, despite adequate warning in some cases, the system becomes no longer stable as it used to be.

"Malware", also known as "scumware", "junkware" or "pestware", is a short form for "malicious software" and normally contains malicious code to accomplish the consciously detrimental intention, once executed, of causing damage to a computer system or data or precluding the authorised users from utilising the system [5]. Another name that can be associated with malware is "crimeware": software used to steal private data or execute other illicit activities, or software that assists in the execution of such conduct. The latter definition of crimeware is also associated with a "warez" site: a site that supplies pirated software and malware, along with hacking manuals. Typical malware threat vectors are "external networks, guest clients, executable files, documents, e-mails and removable media" [6]. In addition, malware has also been designed to infiltrate mobile technologies [7]. One example is the "Symbian malware" (Symbian was discontinued in 2014 due to its inability to compete with the market dominance of iOS and Android [8], which was designed to infect any mobile device which has a Symbian operating system [9].

Malware is notoriously known to be used to initiate Denial of Service (*DDoS)* attacks. However, *DdoS* were thought to be disastrous only to computer programs or data without any direct impairment to the hardware. Just like a biological virus, a computer virus relies on its hosts (computers) to survive [10]. Nevertheless, in 2008, a remote permanent denial-of-service (PDoS) attack, codenamed phlashing, was discovered by Rich Smith, Head of Research for Offensive Technologies & Threats (RiOTT) at HP Systems Security Lab [11]. The term "phlashing" was coined by Rich Smith when he demonstrated his PhlashDance tool to detect and demonstrate PDoS vulnerabilities for the first time at the EUSecWest Applied Security Conference in London on 21 May 2008. PDoS was defined by Rich Smith as "DOS attack requiring the introduction of new hardware, or out of band hardware re-initialisation in order to restore service." He pointed out that

Manuscript received April 5, 2021
Manuscript revised April 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.5.10

most problems stem from the low security profile that is given to firmware, thus the risk needs to be identified at the stage of architecture and development. This is due to the fact that firmware can be poorly set up, and therefore the technical solution is not simple, but multi-layered.

2. The Lurking Danger

The fact that remote control malware, like backdoor, botnet and droneware, can trigger physical destruction is something that needs proper attention [12]. Coupled with "Hardware Destroyers" / "Killer Viruses" [13] and "Stoned Bootkit" the malware-damaging-hardware [14], the aftermath of phlashing goes beyond one" s imagination. Just as internet technology progressed from Web 1.0 up until the recent Web 9.0, the security measure has leaped to an era of Malware 2.0, where the malware operation has evolved from isolated malicious programs to multifarious codes amalgamating with one another [15]. Mustaque Ahamad (2010), a professor at the Georgia Tech Information Security Center (GTISC) stated:

It is known that there are vulnerabilities that would allow cyber criminals to reach into physical systems, and we are aware of the sophistication of today" s attackers, so to think that physical systems are not at risk is really having your head in the sand... As physical systems become more information-driven, the kind of attacks we have seen in other areas will show up here as well. *This is a true concern that requires the collaboration of a wide range of experts, not just technologists, to fully understand and prevent.* (Emphasis added).

3. How The Legal Fraternity Should Respond

When the Computer Crimes Act of Malaysia was passed in 1997, the legal fight against physical damage caused by hacking and cracking activities never crossed the minds of the legislators; hence the provision is silent on this point. This was due to the underestimated perception of the future potential of computer viruses. Such a short sighted perception is unfortunate as legislators are supposed to be exposed to more advanced and structured information before deciding on the framework and wording of legislation. Such underestimation is still common when it involves the general public, as according to a survey conducted by Avira GmbH, a German antivirus software company, in January 2010, computer users take too lightly the risk of illegal access to their computers. The responses from the respondents show that they are concerned about their security but are unsuspecting for the current ingenuity of cyber criminals [16]. The awareness on security has however increased to more than half percentage after a decade, particularly when it involves mobile security [17], eventhough the understanding of the current ingenuity is stillo far from satisfactory. However, when such underestimation comes from the legislators, it is not excusable.

Although the word "impair" is used in the Computer Crimes Act of Malaysia, its meaning under section 2(7) is limited to any event which impairs the normal operation of any computer due to unauthorised modification of computer contents. The old cases of *Cox v Riley* [18] *and R v Whiteley* [19] are useful for the analysis here. In *Cox v Riley*, the court came to the conclusion that the property (the plastic circuit card) had been damaged by the erasure of the computer programs to the extent that the action impaired "the value or usefulness" of the card and "necessitated time and labour and money to be expended" to make the card operable. Wasik (1986) commented on the approach by stating that: "Presumably even in a straightforward case of erasure of data, where the program can easily be recopied from readily available back-up facilities, time or effort of more than a minimal nature would be required." [20]

The court in *R v Whiteley* upheld the decision in *Cox v Riley* and further concluded that the alteration of magnetic particles contained on a non-blank disk, whilst imperceptible, did impair the value and usefulness of the disk and therefore constituted damage. The court made it very clear that while the Criminal Damage Act 1971 of United Kingdom states a condition that there should be an incident of damage to tangible property before a criminal damage can be said to have been committed, the damage itself needs not be tangible in nature. These cases were decided when the Criminal Damage Act and the pre-2006 Computer Misuse Act 1990 complemented one another. Although the Criminal Damage Act did not have any reference to "computer", section 3(6) of the pre-2006 Computer Misuse Act provided that:

For the purposes of the Criminal Damage Act of 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium *impairs* its physical condition. (Emphasis added)

Section 3 of the post-2006 Computer Misuse Act, however has expanded the scope of "impairment":

(1) A person is guilty of an offence if-
(a) he does any unauthorised act in relation to a computer;
(b) at the time when he does the act he knows that it is unauthorised; and
(c) either subsection (2) or subsection (3) below applies.
(2) This subsection applies if the person intends by doing the act-
(a) *to impair the operation of any computer*;
(b) to prevent or hinder access to any program or data held in any computer;
(c) *to impair the operation of any such program or the reliability of any such data;* or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done." (Emphasis added).

With the Computer Crimes Act of Malaysia out of the field, the only way through this malware breakthrough is by returning back to basics by perusing the substantive criminal legislation, namely the Penal Code of Malaysia. But considering its traditional role in dealing with crimes developed in yesteryears, will it be flexible enough for this new breed of terror?

One may argue that the Penal Code of Malaysia provision on damage (termed "mischief" under section 425) may be general enough to cover physical damage caused by malware. But the provisions following it give the impression that the provision was never intended for computer-related mischief. This is because the provisions subsequent to it set very specific examples of the focus and direction of the mischief provision. Section 428 to 440 of the Penal Code of Malaysia provides for mischief involving cattle or any animal, works of irrigation or water diversion, railway, public road, bridge or river, telegraph cable, wire, etc., public drainage, light house, land-mark, fire or explosive substance, vessel and disturbances. There is no single mention of computer or even technology, unless one is bold enough to consider it to be included under the inclusive provision on "telegraph cable, wire, etc" .

However, it should be noted that specific provisions, following their general provisions, are not always to be treated as the sole guide or working illustration of the latter. The maxim *generalia specialibus non derogant* (universal things do not detract from specific things) only applies when there is a conflict between a specific and a general provision because they both contain the same matters, where in that case the former shall prevail. In the case of s 428 to 440, they are simply an expansion of the general "mischief" provision. Furthermore, physical damage caused by malware is not just limited to damage to the invaded computers. A botnet has the capability to manipulate its zombie computers by turning them into machines to initiate destruction on other devices [21]. As far as technical measures are concerned, physical protection, for example, in the form of a hardware anti-virus solution may be adopted [22]. Should not legal protection tally with its technical counterpart?

The use of malware, even if not for phlashing activities, is capable of causing disastrous harm to the amount of memory required for the smooth running of a computer. Spyware, adware, keylogger or screenscaper, once employed, consume memory and processor resources to enable the smooth running of their tracking and monitoring activities [23]. In addition, they consume network bandwidth while establishing a connection with their "headquarters" while running in the background, resulting in a degraded computer performance.

Repeated opening of the CD or DVD tray by a Trojan can cause severe drive failure. The devastation brought by the CIH virus [24] against several hundred thousand computers in 1999, for instance, was so severe that the cost of repairing an infected computer was much higher than the price of a brand new laptop, leading most victims to throw away the computers. Most spectacularly is the Code-Red worm which exploited Microsoft's Internet Information Services" buffer-overflow vulnerability and in pursuance of that infected more than 350000 computers within 24 hours, resulting in more than one billion US dollars in damage [25]. And one always has to bear in mind that malware is not only capable of causing damage to computers, but the computer network as well. For example, an ordinary-scanning-worm-turns-routing-worm has the ability to cause critical clogging in the network [26]. With the rise of 'smart" malware like the self-disciplinary worms which can cause severe damage despite having threshold-based schemes in place [27], having no viable legal solution suited to the problem while ICT experts struggle to set up secure technical measures is like dragging the latter all along to an early surrender to malware.

Based on the above analysis, it is submitted that in terms of reality, as the general impact ranges from cleaning, disinfecting, deleting and reformatting the hard disk, to say that physical damage has not occurred is akin to opening an exit door for malware criminals.

Section 425 of the Penal Code of Malaysia states that:

> Whoever, with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or any person, causes the destruction of any property, or any such change in any property, or in the situation thereof, as destroys or diminishes its value or utility, or affects it injuriously, commits mischief.

There is no reason why the actus reus embodied in the above section cannot be applied to an act of damage caused through malware and badware. The property in question may be the computer itself or any device connected to the computer, but whatever the situation, the chain of malware" s cause and effect is sound and complete. Some computer components are so delicate that any minor physical disturbance will diminish their value or utility.

Therefore, it is imperative that this provision can be used to criminalize any attack or impair to the operation of computer, data program by malware.

The only problem here is whether the provision is sufficient to cover malware mens rea as well. Explanation 1 to the section states that:

It is not essential to the offence of mischief that the offender should intend to cause loss or damage to the owner of the property injured or destroyed. It is sufficient if he intends to cause, or knows that he is likely to cause,

wrongful loss or damage to any person by injuring any property, whether it belongs to that person or not.

Direct prior intention is always at stake when malware perpetrators are employed by others to damage specific targets. However, the application of the phrase, "knows he is likely to cause damage" may differ between the skill levels of the perpetrators and whether they are acting on their own accord or under the specific direction of others. At this point, it would be very appropriate if a test akin to the civil law" s reasonable man test or the principle of constructive notice is applied. As physical damage caused by malware is still relatively new, a test based on the reasonable degree of knowledge on the part of the perpetrators poses a difficult challenge.

3. Conclusion

Nissenbaum stated that: "Within the technical community, the core mission of computer (and network) security, traditionally, has been defined by three goals: availability, integrity, and confidentiality" [28]. These three goals ensure that computer users feel safe and secure while being connected to one another. Unfortunately, the current state of malware's capability ultimately defies these goals. Technical measures have already been developed, but criminals have been able to respond with better technical tactics [29]. Nevertheless, malware is only a tool of the crime.

It is submitted that the current problem is going to stay unless a proper legal measure is taken to eradicate the problem. Nevertheless, whatever the mode of damage is, the end result is always a loss to one party. It does not matter whether the cause of damage is physical or virtual, or whether the damage itself is tangible or nontangible. What matters here is there is one party committing an act of mischief against the other, and the victim has to suffer from that act. Malware attack is a method to destruct or change the property and thus it still falls under section 425 of the Penal Code.

Nevertheless, the enactment of a new section particularly on malware attack is highly recommended. Malaysia should have specific provisions to criminalize any action taken to attack or impair the operation of any computer, data or program. Singapore, for instance, has section 7 of Computer Misuse Act (similar provision with section 3 of the Computer Misuse Act 1990 of the United Kingdom. Malaysia can use this section as a reference.

Law is meant to keep abreast of current technology, otherwise it will have deemed to be obselete in no time. However, one cannot expect for legal provisions to be constantly amended here and then just to keep up with the technological development as logistically and practically speaking, it is not viable and time-consuming. It is even dire when the technogy itself becomes obsolete, as the new technology arrives, the moment the legal process is completed.

Therefore, in addition to amending the legislation, it is also viable if a possible broad interpretation of the provision can be benefited from to cater to justice. Hence the need to always streamline and harmonise the enforcement Standard Operating Procedure in dealing with the problem.

Acknowledgments

The research leading to the publication of this article is funded by a research grant from Universiti Kebangsaan Malaysia (DPK-2019-002).

References

[1] Virgil and Mandelbaum, A. (translator), *The Aenied of Virgil*. 35th ed. Berkeley, University of California Press, 2007.
[2] Trusted Integrated Circuits (TRUST). Defense Advanced Research Projects Agency, 2008, http://www.darpa.mil.
[3] Stokes, J. Pentagon Fears Trojans, Kill Switches In Foreign-Made CPUs. *ArsTechnica*. http://arstechnica.com [2 May 2008]
[4] Navarro, P. and Autry, G. *Death by China: Confronting the Dragon - A Global Call to Action*. Upper Saddle River, Prentice Hall, 2011.
[5] Freedman, A. *Computer Desktop Encyclopedia*. eBook edition. Osborne/McGraw-Hill, 2014.
[6] Malware Defense Guide, 2011. http://technet.microsoft.com.
[7] Dunham, K. (ed). *Mobile Malware Attacks and Defense*. Burlington, Syngress Publishing, 2009.
[8] The Symbian Foundation Community http://www.symbian.org.
[9] Threat Encyclopedia. Trend Micro, 2021. https://www.trendmicro.com/vinfo/us/threat-encyclopedia
[10] Boase, J., Wellman, B. A Plague of Viruses: Biological, Computer and Marketing. *Current Sociology*, 49(6), 39, 2001.
[11] Smith, R. Phlashdance: Discovering Permanent Denial of Service Attacks against Embedded Systems. Presentation Slides. EUSecWest, 2008. http://eusecwest.com.
[12] Trojans Suspected of Contributing to 2008 Madrid Aircrash. *Infosecurity*, 8, 2010. http://www.infosecurity-magazine.com.
[13] Kizza, J. M. *A guide to Computer Network Security*. Chattanooga, Springer, 2009.
[14] Kleissner, P. Stoned Bootkit. 2010. http://www.stoned-vienna.com.
[15] Malware Evolution in 2007. Kaspersky Security Bulletin, 2007. http://www.kaspersky.com.
[16] Avira. http://www.avira.com [December 2010].
[17] Mobile Security Report. Avira, https://www.avira.com/en/mobile-security-report [November 2020].
[18] (1986) 83 Cr App R 54.

[19] (1991) 93 Cr App R 25.
[20] Wasik, M. Criminal Damage and the Computerised Law. *New Law Journal*, 136(6266), 763, 1986.
[21] Chao, L, Wei, J. and Xin, Z. Botnet: Survey and Case Study. *IEEE Computer Society*, 1184, 2009.
[22] Gao, Q., Hu, Y., Li, L., Chen, X. and Liu, H. A Novel Computer Architecture to Prevent Destruction by Viruses. *J. Comput. Sci. & Technol*, 17(3), 241, 2002.
[23] Baskin, B. et al. *Combating Spyware in the Enterprise*. Rockland, Syngress Publishing, 2006.
[24] "W95/CIH-10xx" Sophos http://www.sophos.com.
[25] Lemos, R. Virulent Worm Calls into Doubt Our Ability to Protect the Net. CNET News, 2001. http://news.cnet.com.
[26] Zou, C. C., Towsley, D., Gong, W. & Cai, S. Advanced Routing Worm and Its Security Challenges. *SIMULATION*, 82(1), 75, 2006.
[27] Wei, Y., Nan, Z., Xinwen, F. & Wei, Z. Self-Disciplinary Worms and Countermeasures: Modeling and Analysis. *IEEE Transactions on Parallel and Distributed Systems*, 21(10), 1501, 2010.
[28] Nissenbaum, H. Where Computer Security Meets National Security in Balkin, J. M., Grimmmelmann, J., Katz, E., Kozlovski, N., Wagman, S., and Zarsky, T. (eds). *Cybercrime: Digital Cops In A Networked Environment*. New York, New York University Press, 2007.
[29] Gissel, R. *The Development and Evaluation of a Computer Crime Investigative Distance-learning Program for the National Cybercrime Training Partnership*. New York, MacroTech Press, 2005.

Rizal Rahman is an Associate Professor of Law at the Faculty of Law, Universiti Kebangsaan Malaysia with 24 years of experience in the legal fraternity. His areas of expertise are Information Technology Law, Evidence Law, Constitutional and Administrative Law, and Business Law. He is also the Chairman of Malaysian and Comparative Law Centre (http://www.ukm.my/cmcl).

Mohd Sophian Zakaria is a Deputy Public Prosecutor at the Attorney General's Chambers of Malaysia with 17 years of experience in the legal fraternity. His areas of speciality include Cyber Law, Evidence Law and Commercial Crimes Law. He is the author of a book titled Social Media Offences: Investigation and Prosecution Manual.