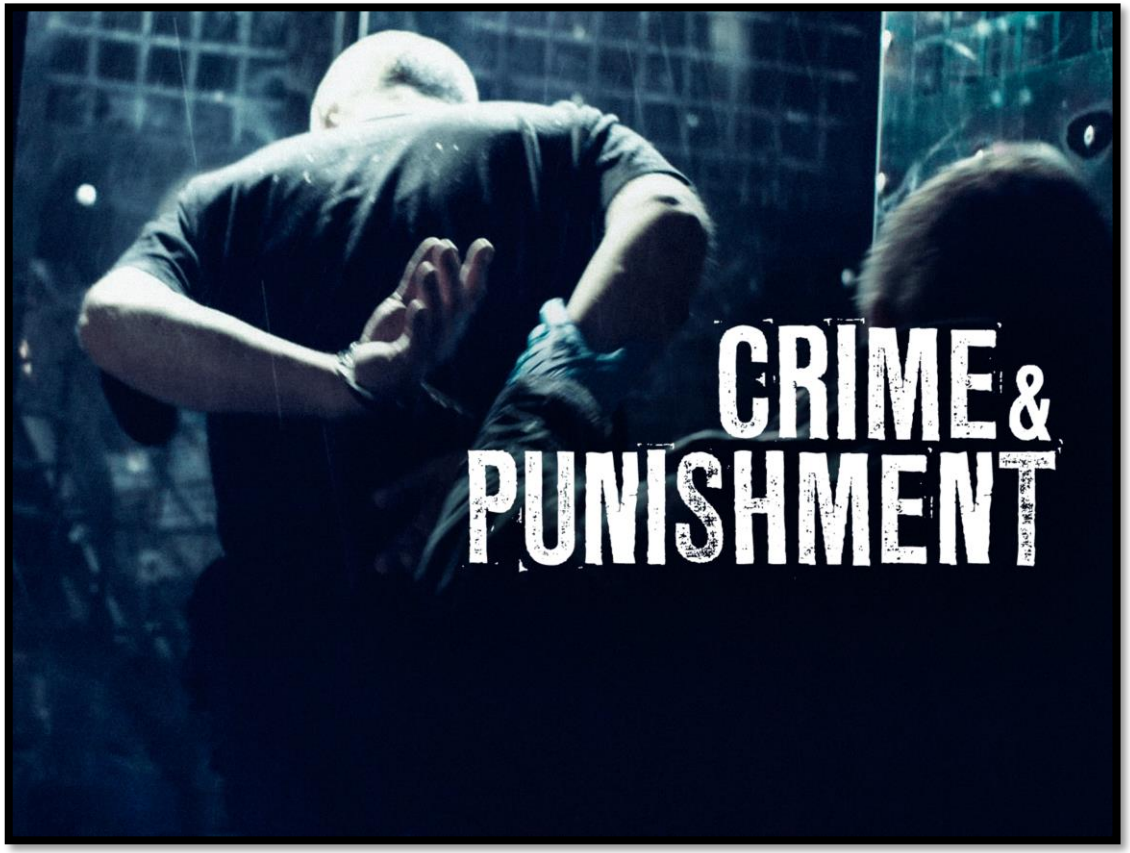
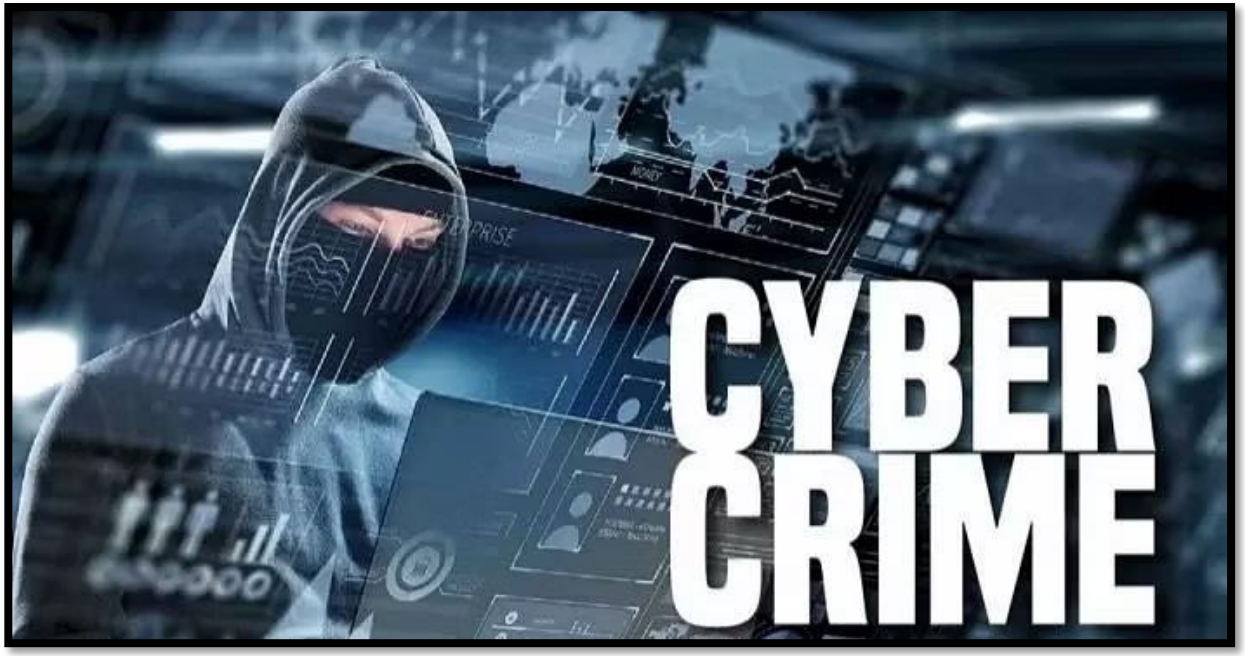


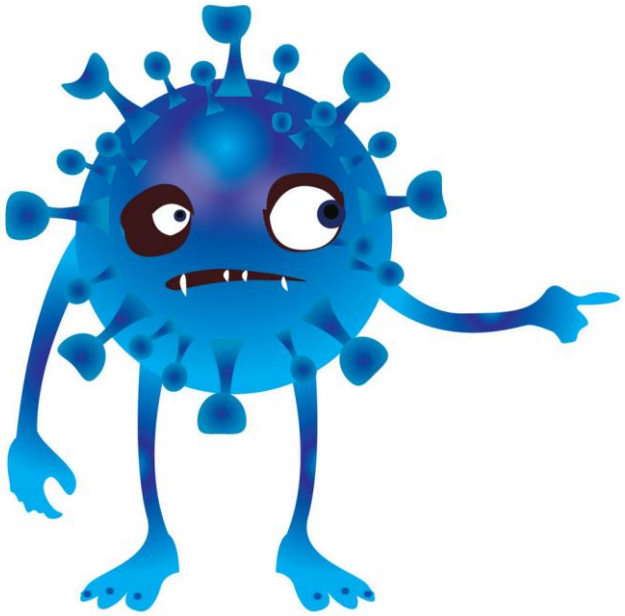
Chapter 9
Online Crime and Real Punishment

Table of Contents



Malware Crime

Malware crime refers to the illicit activities carried out through the use of malicious software, commonly known as malware. It involves the creation, distribution, and deployment of harmful software with the intention of causing damage, unauthorized access, or financial gain. Malware can take various forms, including viruses, worms, ransomware, spyware, and Trojans, and can be spread through infected files, email attachments, malicious websites, or vulnerable software systems.



Malware criminals exploit vulnerabilities in computer networks, systems, and devices to compromise security, steal sensitive information, engage in identity theft, conduct financial fraud, or disrupt essential services. These criminal acts can result in financial losses, privacy breaches, reputational damage, and even pose risks to national security.

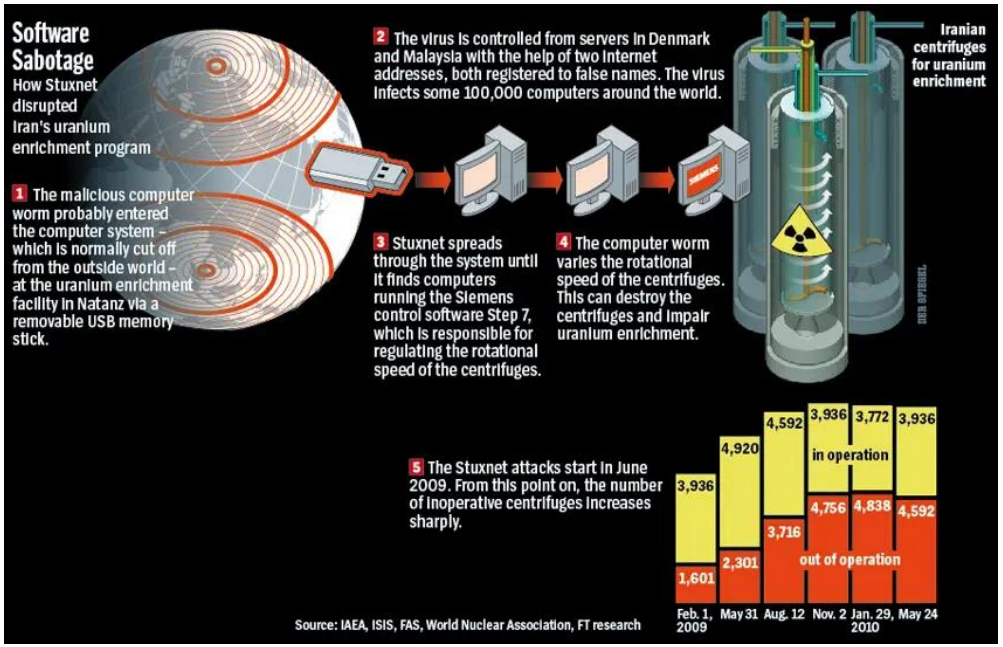
Additionally, law enforcement agencies and international collaborations play a vital role in investigating and prosecuting individuals involved in malware crime, aiming to deter such activities and protect individuals, organizations, and the digital infrastructure from the damaging effects of malicious software.

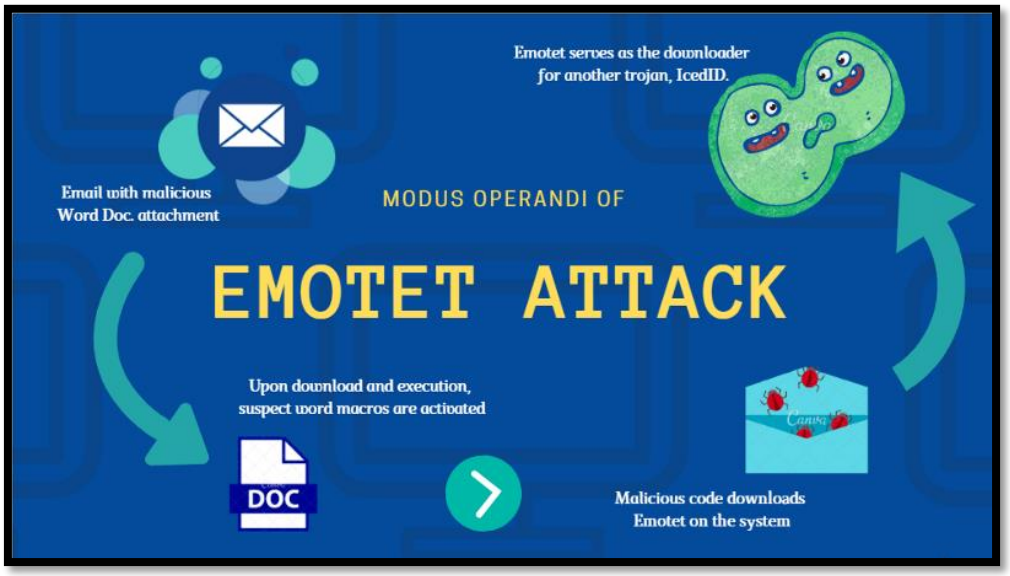
Malware Crime

Distribution of Malware
Malware Infections
Botnets and Command & Control (C&C) Networks
Ransomware Attacks
Phishing and Social Engineering
Data Theft and Unauthorized Access
Identity Theft and Fraud
Distributed Denial of Service (DDoS) Attacks
Exploiting Software Vulnerabilities
Malvertising (Malicious Advertising)
Keylogging and Password Theft
Cryptojacking (Unauthorized Use of Computing Resources for Cryptocurrency Mining)
Adware and Spyware
Advanced Persistent Threats (APTs)
Malicious Mobile Apps

Malware crimes that have been caught in the past:

Stuxnet (2010)
Conficker (2008)
Zeus Trojan (2007-2010)
CryptoLocker (2013)
WannaCry (2017)
Mirai Botnet (2016)
NotPetya (2017)
Carbanak/Anunak (2013-2015)
GameOver Zeus (2014)
Emotet (2014-2021)





Potential punishments for malware crimes:

Imprisonment
Fines
Restitution
Probation
Asset seizure
Community service
Court-ordered computer restrictions
Mandatory counseling or rehabilitation programs
Restraining orders
Loss of computer or internet privileges
Civil lawsuits for damages
Professional and reputational consequences

Malware Case in Malaysia

One notable malware case in Malaysia is the "Love Bug" or "ILOVEYOU" malware incident. This malware attack occurred in May 2000 and affected computer systems worldwide, including those in Malaysia.

The Love Bug malware spread through email attachments with enticing subject lines, leading users to open the infected file. Once opened, the malware would overwrite files, steal passwords, and spread itself to the user's contacts.

The Love Bug malware caused significant disruptions in Malaysia and globally, affecting government agencies, businesses, and individuals. It led to the loss of critical data, financial damages, and operational disruptions.

Computer security

Computer security refers to the protection of computer systems, networks, and data from unauthorized access, use, disclosure, disruption, or destruction. It encompasses various measures, practices, and technologies designed to safeguard the confidentiality, integrity, and availability of digital information.

Computer security involves implementing robust defenses against cyber threats, such as malware, viruses, hackers, and data breaches. This includes the use of firewalls, antivirus software, encryption, strong passwords, and access controls. Additionally, computer security emphasizes the importance of user awareness and education to mitigate risks associated with social engineering, phishing, and other forms of cyber attacks.

Proactive monitoring, incident response planning, and regular security updates are vital components of maintaining computer security. By establishing and maintaining effective computer security measures, individuals and organizations can protect sensitive information, preserve privacy, prevent financial losses, and ensure the smooth functioning of digital systems.

Laws against computer misuse

Computer Fraud and Abuse Act (CFAA) (United States): The CFAA is a federal law that criminalizes various computer-related offenses, including unauthorized access, fraud, and the distribution of malicious software. It also covers activities such as trafficking in passwords, extortion, and the unauthorized access of protected computers.

Computer Misuse Act (United Kingdom): The Computer Misuse Act is a UK legislation that criminalizes unauthorized access, modification, and disruption of computer systems. It covers offenses such as hacking, distributing malware, and using or creating tools for illegal purposes.

Act on the Protection of Personal Information (Japan): This law in Japan regulates the handling and protection of personal information, including data stored in computer systems. It sets standards for collecting, storing, and processing personal data and imposes penalties for unauthorized access, leaks, or misuse of personal information.

Cybercrime Prevention Act (Philippines): This law addresses a wide range of cybercrimes, including offenses related to hacking, identity theft, fraud, and cybersex. It provides for penalties and legal mechanisms to combat cybercrimes and protect computer systems and data.

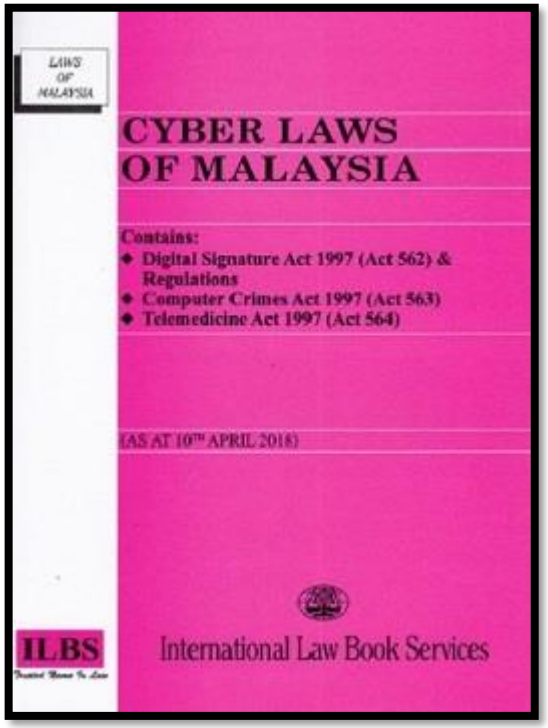
Criminal Code Amendment (Computer Offences) Act (Australia): This law amends the Australian Criminal Code to include offenses related to unauthorized access, modification, or impairment of computer systems. It also addresses activities such as unauthorized interception of data, forgery, and unauthorized disclosure of protected information.

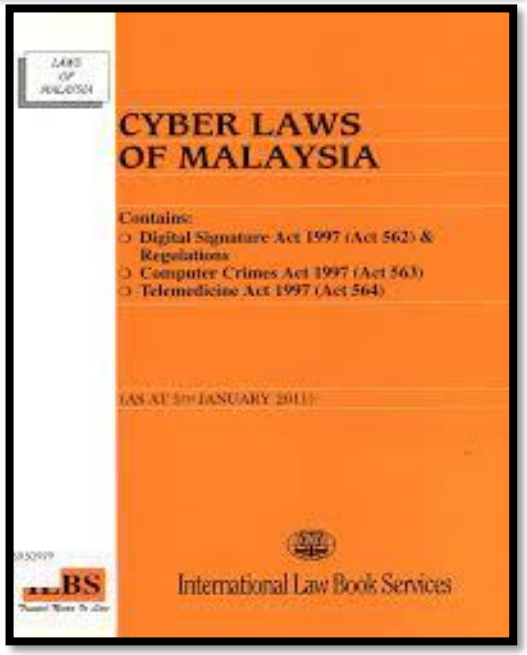
Information Technology Act (India): The Information Technology Act addresses various cybercrimes in India, including unauthorized access, hacking, data theft, identity theft, and the distribution of obscene or offensive material. It provides legal provisions and penalties for offenses committed through electronic means.

Data Protection Act (European Union): The Data Protection Act (DPA) is a regulation that aims to protect the privacy and security of personal data within the European Union (EU). It sets standards for the collection, processing, and storage of personal data and imposes penalties for breaches of data protection principles.

Cyberlaws of Malaysia

- Computer Crime Act 1997
- Communications And Multimedia Act 1998 (CMA)
- Malaysian Communications And Multimedia Commission Act 1998
- Digital Signature Act 1997
- Copyright Act (Amendment) 1997
- Telemedicine Act 1997
- Optical Disc Act 2000
- Electronic Commerce Act 2006



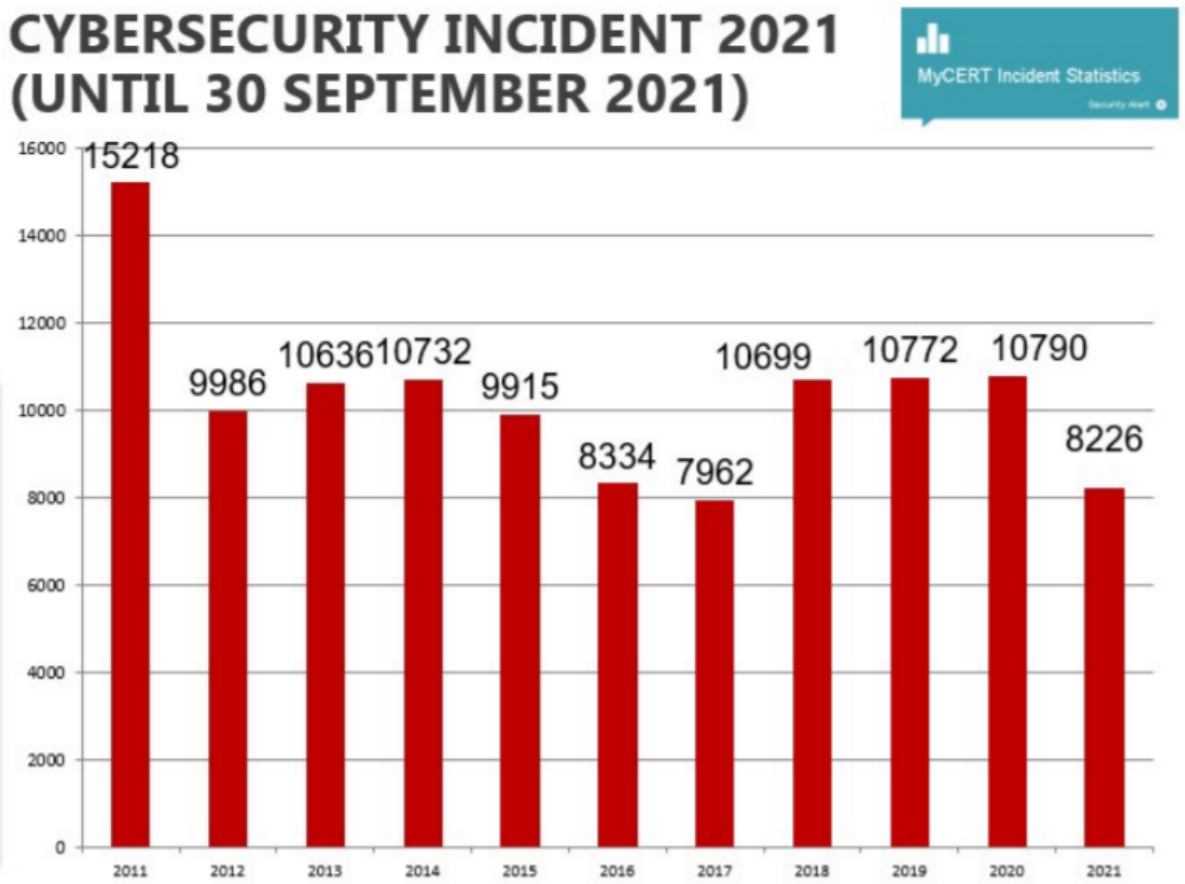


Cyberlaws of Malaysia

MyCERT
Malaysia Computer Emergency Response Team

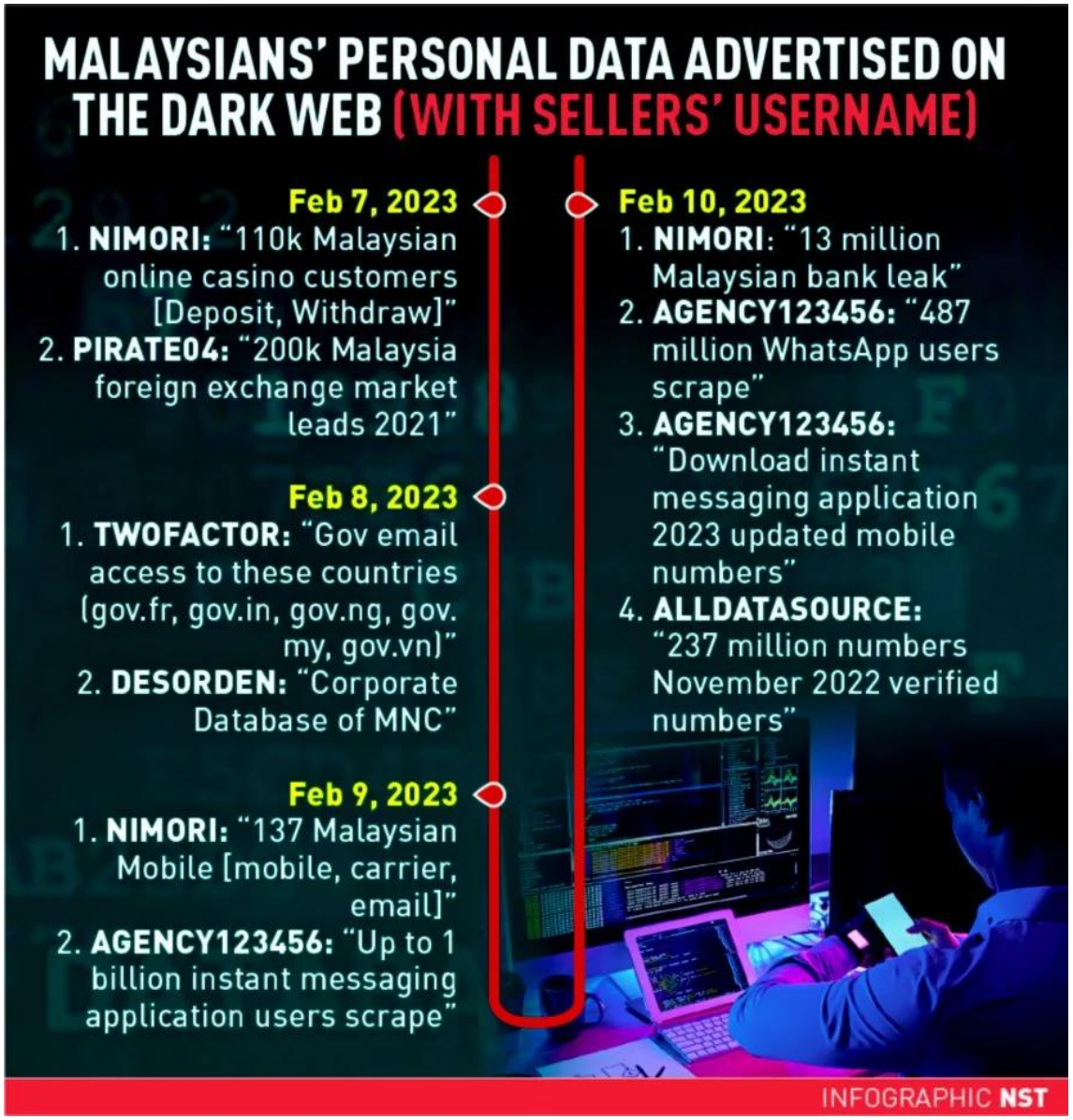
Type of Incident (Except Spam)

1. Denial of Service
2. Vulnerabilities Report
3. Malicious Codes
4. Cyber Harassment
5. Fraud
6. Intrusion Attempt
7. Content Related
8. Intrusion
9. Spam



Cyberlaws of Malaysia

Cyberlaws of Malaysia



Cyberlaws of Malaysia

End