CybercrimeModus Operandi: Computer Misuses

Abstract

The problem in the cybersecurity is how to interpret and determining the cybercrime modus operandi. Most of investigators and cybersecurity professionals have a limited understand on how the cybercriminals plan, organize and commit their crimes. Also, most of investigators are have limited knowledge and skills on the objectives, techniques, tools, tricks or traps and determinants of the cybercriminals. This study applied the Systematic Literature Review (SLR) which is a robust methodology to collect, identify, and critically analyze the available research studies, such as a articles, conference proceedings, books, dissertations, through a systematic procedure. This study define the modus operandi as *the dynamic learned specific or unique means, characteristic, action or behavior possessed or shown by the cyber attacker in entering, executing, exiting and escaping from the crime scene; it involves all techniques, tools, psychological and technical tricks applied by cybercriminals before, during and after the cyber-attack.*The study finding that the common and effective cyberattack tricks are psychological tricks such are fears, familiarity, urgency, trust, emotional appeal, curiosity. These psychological trick are crafted to deceive the users on the cyber attacker psychological trick phrases send through their email or mobiles. The study conclude that most of the cyberattacks start with the phishing attacks which uses both psychological and technical tricks. Moreover, the psychological tricks are more effectively than technical tricks. Hence, the study recommended the application of protection or anti-psychological and anti-technical trick techniques such as uses of strong passwords, two factor authentication (2FA), antivirus, cybersecurity training, firewalls, incident response plans, employee training, security audits, threat intelligence, secure payment gateways, SSL/TLS, data encryption, Multi-factor authentication, cybersecurity awareness programs, strong cybersecurity policies and strong network segmentation.

Keywords: Cybercrime, modus operandi, phishing attack, psychological tricks, technical tricks

Introduction :

1.0 Background and Literature Review

Modus operandi (MO) is a Latin term that means method of operating (Turvey, 2013). It refers to the manner in which a crime has been committed (Turvey, 2013; Woodhams et al., 2007). It is comprised of acts and decisions that are necessary to commit a crime, and any related choices made by an offender. In other words, the term modus operandi refers to the specific offender behaviors at crime scenes, the offender's courses of action while performing the crime because it is assumed that individual offenders to various extents commit their crimes in similar ways (Sundberg, 2020).On the other hand, crime scene behaviors such as how close crime incidents occur in time and space, how criminal have entered premises, factors for selecting targets and type of goods that have been stolen have been identified as relevant linking features whose predictive accuracy for crime linkage are necessary to evaluate(Turvey, 2013; Sundberg, 2020).

Law enforcement has long held to the belief that understanding the methods and techniques criminals use to commit crime is the best way to investigate, identify, and ultimately apprehend them (Turvey, 2013; Sundberg, 2020). An offender's MO behaviors are learned, and by extension they are dynamic and malleable (Turvey, 2013). This is because MO is affected by time and can change as the offender learns or deteriorates. MO is not consistently comprised of behaviors that are necessarily distinctive or even unique to a particular offender; their crimes will often unfold differently each time, even when committed with the same motive, intent, and methods (Turvey, 2013). MO is best used to help guide investigators to more certain evidence and keep their efforts on course (Turvey, 2013). It should not generally be confused as conclusive evidence suggestive of offender identity when two or more cases are being compared, and certainly not in a legal context (Woodhams et al, 2007).

Some studies states that crime linking through modus operandi is an adequate method for assisting police investigations, but that perfect predictions cannot always to be expected (Sundberg, 2020, Woodhams et al., 2007). Sundberg (2020) and Woodhams et al. (2007) urged that the false positive as well as false negative predictions will inevitably be made if we link MO and criminal. Therefore, the purpose of crime linkage is to guide or complement investigations rather than provide evidence (Sundberg, 2020). The research on crime linkage through behavioral aspects extends across various crime types, originally sexual offences, and homicide but also volume crimes such as different types of theft, robbery, or burglary and now cybercrime. Some studies contended that the best predictor for linking series of crimes to one offender is forensic evidence such as DNA or fingerprints (Sundberg, 2020; Tonkin et al, 2011; Woodhams et al, 2007).Crime linkage through behavioral factors have been of interest within police forces in different countries for several years and is sought to complement the available information of hard forensic evidence such as DNA or fingerprints, which may not present at crime scenes. Forensic evidence is regarded as reliable information for linking series of crimes as well as evidence leading to convictions, but it has also been described as time consuming and expensive, alongside the fact that it can be difficult to get access to on many crime scenes (Woodhams, 2007).

Recently, the emergency of the modern crimesthat are committed by computer and information technologies such as cybercrimes, poses a challenge for traditional investigators on how to identify and map for modus operandi of those crimes, particularly, the cybercrimes. This is because, the cybercriminals hide their behavior or techniques of committing crimes, and unluckily, they are skilled on technology and computer applications. Understanding the modus operandi of the cybercriminals is an emergency concern in developing effective cybersecurity strategies (Pospisil, 2020).Cybercriminals employ a variety of techniques to compromise systems, steal sensitive information and exploit vulnerabilities (Pospisil, 2020; Tonkin et al, 2011).Modus operand of cybercrime is still questioned as the changing and rapid proliferation of technology, and the cybercriminalsquickly ortimely changing to or adapting the new technology.This is become a challenge for the cybercrime investigators. Unfortunately, the studies on modus operandi of cybercriminal is still limited to the researchers who are skilled on ICT.

Due to this, fact, this study aimed to introduce a new concept of interpreting and determining the modus operandi of the cybercriminals. The study introduced the new definition of the cybercrime modus operandi to include techniques, tools, trick, objective and determinants of the cybercriminals. Notably, in this paper we discussed the cybercrime modus operandi by encompasses the objective, techniques, tools, trick and the determinants of the cybercriminals.

Therefore, the study of the cybercrime modus operandi by using this approach will help the investigators and the decision makers to set the proper cybersecurity solution theirregions or organisations. Moreover, this study described the cybercrime countering or protection techniques for each cybercrime modus operandi. This is very help because it provides the awareness skills on both investigators and other cybersecurity professionals torid of from the risk of cyber-attacks. Moreover, the paper provides the systematic stage of cybercrime attacking model from intent stage to the impact stage or phase. This also, help the investigators and other cybersecurity professionals to understand how the cybercriminals are planning, organizing and attacking their target. On the other hand, the paper described the main vulnerable targets of the cybercriminals with their respectively goals and modus operandi.

This paper applied the systematic literature reviews (SLR) methods to compile and analysis the theoretical and empiricalacademic, professional and technical studies and reports to enhance the findings. The next part of the paper covers the cybercrime and its categories, methodology, finding, discussion and conclusion and recommendation.

2. Cybercrime and its Categories

To get clear understanding on the cybercrime, we use the common ways of classification or categorization of traditional crimes. Therefore, we can categorized the cybercrime in four (4) categories, namely cybercrimes against individuals (CAI) such as E-mail spoofing, spamming, phishing, social engineering,cyber defamation, cyber harassments and cyber stalking(ProofPoint, 2024). The second class is the cybercrime against property (CAP) which include credit card frauds, internet time theft and intellectual property crimes (TTU, 2024; ProofPoint, 2024). The third class is the cybercrime against organizations (CAO) which include unauthorized accessing of computer, denial of service, computer contamination / virus attack, e-mail bombing, Man –in-the Middle (MITM),salami attack, logic bomb, trojan horse and data diddling(ProofPoint, 2024). And the fourth class is the cybercrime against society (CAS) which include forgery, cyber terrorism, web jacking and cyberwarfare (TTU, 2024).

Email spoofing is a technique used by cybercriminals to forge the sender's address on an email, making it appear as though it is coming from a trusted source(TTU, 2024; Pandey, Kumar, and Singh, 2017; FIA, n.d). This is often done to trick recipients into revealing sensitive information or to spread malware (TTU, 2024). For example, an attacker sends an email that appears to be from a well-known bank, warning the recipient that their account will be suspended unless they click a link and verify their information. The spoofed email that looks like it’s from a company executive requesting a wire transfer to a fraudulent account (Pandey et al., 2017; FIA, n.d). The spamming refers to the practice of sending unsolicited messages, typically in bulk, to a large number of users (TTU, 2024;ProofPoint, 2024). These messages can be promotional, malicious, or deceptive in nature (ProofPoint, 2024). For examples, the individual or organization receiving numerous emails advertising products or services that you did not sign up for, often containing links to dubious websites. The attacker usually use the psychological tricks such as sending spam messages that promote scams, such as "get rich quick" schemes or fake lottery winnings (TTU, 2024; Li and Liu, 2021).

3. Problem in CybercrimesInvestigations

The problem in the cybercrime investigation is how to interpret and determining the cybercrime

modus operandi. Most of investigators and cybersecurity professionals have a limited understandon how the cybercriminals plan, organize and commit their crimes. Also, most of investigators are have limited knowledge and skills on the objectives, techniques, tools, tricks or traps and determinants of the cybercriminals. Moreover, the investigator have a little knowledge on how to protect themselves and the community from cyber-attacks. Cybercriminals are always advancing with a new technology. In most case, the cybercriminals have both financial and technology capacity, hence they can influence the investigation process by application of technological skills and financialcapacity they have. They can buy or develop cybercrime technique and tools easily. Unlucky, in some cases the investigators were limited on the budget, so it can a challenge for investigator to get tools for cybercrime countering. This is because, most of the cybercrime penetration or investigation tools are more expensive.

On the other words, Tundis et al., (2020) supports that sometime investigator can be limited with knowledge on how the crime committed (cybercrime modus operandi), this is because the cybercrimes are committed with *the people with specialized knowledge*. Cybercrimes can only be committed through the technology, thus to commit this kind of crime one has to be very skilled in internet and computers to commit such a crime. If the investigator is limited or has no knowledge about the technology used to commit the crime, the investigator will do nothing! The people who have committed cybercrime, in most cases are well educated and have deep understanding of the usability of internet, and that's made work of police machinery very difficult to tackle the perpetrators of cybercrime (Tundis et al., 2020). That is, we need a comprehensive study on cybercrime modus operandi to disclose the target objectives, techniques, tools, trick and traps and determinants of the cybercriminals, to help the investigators and other cybersecurity professional to set appropriate cybersecurity plans. This is done by this paper.

4.Study methodology

The study applied the Systematic Literature Review (SLR). SLR is a research methodology to collect, identify, and critically analyze the available research studies, such as a articles, conference proceedings, books, dissertations, through a systematic procedure (Carrera-Riveraa et al., 2022; Pati and Lorusso, 2018). An SLR updates the reader with current literature about a subject-cybercrime modus operandi (Carrera-Riveraa et al., 2022; Kitchenham and Charters, 2007). The goal is to review critical points of current knowledge on a cybercrime about the modus operandi to suggest areas for further examination (Carrera-Riveraa et al. 2022). The study used the PICOC (Population, Intervention, Comparison, Outcome, and Context) criteria to break down the SLR's objectives into searchable keywords and help formulate research questions (Yang et al., 2021). PICOC is widely used in the medical and social sciences fields to encourage researchers to consider the components of the research questions (Yang et al., 2021; Wohlin et al., 2012). This methods helped a researcher to organized research questions by considering the PICOC criteria. Furthermore, the researcher applied the PSASAR (protocol, Search, Appraisals, synthesis, analysis, report) framework which is developed from SASA (Search, Appraisal, Synthesis, and Analysis). The framework of Search, Appraisal, Synthesis, and Analysis (SASA) is a methodology to determine the search protocols which the SLR should follow (Mengista, Soromessa and Legese, 2020). SASA guarantees methodological accuracy, systematization, exhaustiveness, and reproducibility. Most studies applied this methodological approach to reduce risks related to publication bias and to increase its acceptability of the work (Mengista et al., 2020; Yang et al., 2021; Wohlin et al., 2012). This PSASAR framework of SLR work, therefore, applied six steps which are protocol, Search, Appraisals, synthesis, analysis and report. This study applied this method purposely to extract the

intended theme from both theoretical and empirical studies.

5. Findings

This study aimed to introduce a new concept of interpreting and determining the modus operandi of the cybercriminals. Therefore, theintroduced the new definition of the cybercrime modus operandi to include techniques, tools, trick, objective and determinants of the cybercriminals. Moreover, this study described the cybercrime countering or protection techniques for each cybercrime modus operandi. In addition, the paper provides the systematic stage of cybercrime attacking model from intent stage to the impact stage or phase.

5.1 Definition and Interpretation of MO of Cybercrime

According to Turvey (2013), an offender's MO behaviors are learned, and by extension they are dynamic and malleable, and MO is affected by time and can change as the offender learns or deteriorates. TheModus operandi (MO) is a Latin term that means "method of operating" (Turvey, 2013). MO refers to the *manner* in which a crime has been committed (Turvey, 2013; Woodhams et al., 2007). It is comprised of *acts and decisions* that are *necessary* to commit a crime, and any related choices made by an offender. Furthermore, the MO is related to means and techniques used by the criminal to enter and leave the scene of crime (Sundberg, 2020). These studies lack its completeness on the nature of the cybercrime. They describe the traditional crimes such as rape and burglary. For example, Turvey (2013) agree that MO change with time, but overlook the time is always associate with the technology changes. Moreover, the literature explains only the modus operandi as the manner on how crime was committed, overlook how the criminal entered and escaping from scene of crime. Therefore, this paper fills the theoretical gap on the definition and interpretation of cybercrime modus operandi in the cyberspace.In that sense, we extract fact that, *what the criminals do at the crime scene is the modus operandi determined by their prior and after (post) plans.* The prior and after (post) plans influences the modus operandi. The cybercriminals plan comprises of targets, objectives, tools, trick or traps and risk assessment report basing on three planning stages, prior, during and post (after) the event.

Therefore, we define the *modus operandi in the cyberspace as the dynamic learned specific or unique means, characteristic, action or behavior possessed or shown by the cyberattacker in entering, executing, exiting and escaping fromthe crime scene; it involves all techniques, tools, psychological and technical tricks applied by cybercriminals before (prior), during and after(post) the cyber-attack*. This is mostly influenced by the time and technical changes. For example, some cybercriminals cover their faces during the cyber-attack. In that sense, when we term modus operandi in the cyberspace we mean all techniques, tools, trick and traps that cybercriminals are applied.

5.2 Cyber Attacking Stages and their Modus Operandi

The study provided a full descriptions on how the cybercriminals plan, organize and attack to the selected targets. The study provided the objectives, techniques, tools, trick or traps, and determinants of the cybercriminals at each stage or phase of the attack. The study identified 8 stages or phases taken or followed by a cybercriminal to attack their target.

5.2.1: Intention or contemplation phase

The first stage in the commission of a cybercrime is to contemplate its commission. This is thestage where the intention to commit a crime germinates in the minds of the offender and takes a concrete shape. This is the mental state which is generally described subsequently as the requisite *mens rea* to commit an offence (Wall, 2015). In criminal law, intent is define as a determination to perform a particular act or to act in a particular manner for a specific reason (Dressler, 2015). It is the mental aspect of a crime that is often necessary to criminally prosecute a defendant (Simester and Sullivan, 2016). A person's intent demonstrates that he or she knew what the likely outcome of his or her crime would be before committing it and desired that outcome (Herring, 2018). This guilty mind or mens rea, is one of the main criminal elements that must be proven to convict someone of a crime. The majority of crimes rely on intent in order for a defendant to be found guilty of criminal behavior (Ashworth, 2013). Criminologist distinguish specific and general intent. The specific intent refer to the particular state of mind in which the defendant not only intendent to commit an actus reus or guilty act (the second required element), but he must also have intendent the consequences of that act (McAuliffe, 2017). It is a way to define a case in which the defendant intendent all elements of the crime at hand. General intent crimes are simply the intent to do what is forbidden by law. The prosecution does not have to prove the defendant intended everything that unfolded from committing the crime.

5.2.2: Reconnaissance and Compromise Phase

Reconnaissance and compromise, or footprinting is the second period prior to an attack which criminals researching and gathering information about the target organization(Surya et al., 2023; Naushad and Ajaz, 2022). It is the preparatory phase where the cybercriminals collect as much information and intelligence as possible about the target(Surya et al., 2023; Naushad and Ajaz, 2022).They usually collect information and intelligence about three groups which are network, host and entity (people or organisation) (Pospisil, 2020).This process involves the collection techniques of publicly accessible data, facilitating an in-depth comprehension of the target's technological infrastructure, system architecture, and potential security vulnerabilities (Surya et al., 2023; Naushad and Ajaz, 2022). The primary objective at this stage is to construct a comprehensive profile of the target, enabling cybercriminals to pinpoint potential entry points for subsequent penetration testing or cyberattack (Surya et al., 2023; Naushad and Ajaz, 2022). At this phase, criminals look for network ranges, IP addresses and domain names. The cyber attackers also try to find the email addresses of key players in an organization, or identify vulnerable employees by sending phishing emails. There are two types of foot printing which are Active and Passive (Surya et al., 2023). Active is cybercriminal directly interacting with the target to gather information about the target. E.g., using Nmap tool to scan the target. The Passive foot printing, cybercriminal trying to collect the information about the target without directly accessing the target. This involves collecting information from social media, public websites etc. the common collection methods at this stage in either passive or active are OSINT (Open source intelligence) and WHOIS Lookups (Naushad and Ajaz, 2022; Pospisil, 2020). OSINT is intelligence collection methods that leveraging publicly available sources of information, such as public records, domain registration details, and social media profiles, to build a comprehensive profile of the target.WHOIS Lookups is the methods which is querying WHOIS databases to obtain information about domain ownership and registration details (Naushad and Ajaz, 2022; Pospisil, 2020).

5.2. 3: Scanning the Target Phase

After accessing the network, host and people involved criminals try to infiltrate further into the network by acquiring access privileges (CCEPL, 2024; Surya et al., 2023). Attackers scan the target

to see or checks the weakness or vulnerability of the targets (Chandran, 2023). The scanning helps the cyber attackers to select the proper or appropriate target to attack or to penetrate (EC-Council, 2024). There are three types of scanning that done by cybercriminals which are port scanning, vulnerability scanning and network mapping (Surya et al., 2023, Naushad and Ajaz, 2022). Port scanning is the phase that involves scanning the target for the information like open ports, live systems, and various services running on the host (Naushad and Ajaz, 2022). Vulnerability Scanningis the checking the target for weaknesses or vulnerabilities which can be exploited (Pospisil, 2020). Usually done with help of automated tools such as metasploit, Nmap (Network Mapper), Nessus, Nikto. Metasploit is a penetration testing framework that includes various modules for scanning, exploiting, and post-exploitation activities (CCEPL, 2024); Surya et al., 2023). It's used to identify and exploit vulnerabilities. Nmap is a versatile and widely-used open-source tool for network discovery and security auditing (Chandran, 2023). It excels in port scanning, service detection, and OS fingerprinting. Network Mapping is the finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information(EC-Council, 2024; Pospisil, 2020). This map may serve as a valuable piece of information throughout the hacking process.

5.2. 4: Gaining Access Phase

Gaining access for cybercriminal is a systematic process of exploiting previously identified vulnerabilities. This phase involves executing precise technical actions to gain entry into the target system or network (Naushad and Ajaz, 2022). The primary objectives of gaining access may include stealing sensitive information such as personal data, financial records, or intellectual property (Data theft), gaining control over systems to launch further attacks or maintain a presence (System control) and causing service interruptions or damage to systems (Disruption). This stage is critical as it allows the cybercriminal to maneuver within the system, execute commands, and potentially carry out malicious activities such as data theft, installation of malware, or further exploitation (EC-Council, 2024).

In this stage the criminals do exploitation of vulnerabilities to identify and exploit weaknesses in software, hardware, or network configurations (CCEPL, 2024; Surya et al., 2023). This can involve exploiting known vulnerabilities or misconfigurations. The common techniques used are phishing, Brute Force Attacks, SQL Injection, Social Engineering and Pharming and DNS Spoofing (EC-Council, 2024; Surya et al., 2023). Phishing is techniques that are tricking users into revealing credentials.Brute Force Attacks isa systematically guessing passwords until the correct one is found (Surya et al., 2023).SQL Injection is where the cybercriminal is manipulating database queries to gain access to data or bypass authentication, the Social Engineering is a process where a criminal Manipulates individuals into providing access or sensitive information, and Pharming and DNS Spoofing are techniques involve redirecting network traffic to malicious servers, tricking users or systems into connecting to unauthorized resources (EC-Council, 2024; Naushad and Ajaz, 2022).

.

5.2.5: Maintaining Access Phase

Maintaining access or Persistence is a crucial stage in the cybercriminal attack process where attackers establish a persistent foothold in a compromised system or network(CCEPL, 2024).The main goal of maintaining access is to ensure that the attacker can continue to exploit the system for

data exfiltration, further attacks, or other malicious activities without needing to re-exploit the initial vulnerability (Surya et al., 2023). In other words, this allows the attackers to return to the system at will, even after initial vulnerabilities are patched or discovered(CCEPL, 2024; Surya et al., 2023).This phase involves various tactics and techniques to ensure continued control over the compromised system or network, replicating real-world attacker persistence to assess the potential risks and impact on the target (Naushad and Ajaz, 2022). The common techniques at this stage are backdoor installation, credential harvesting, Rootkits, creating User account, Privilege Escalation, Persistence Scripts, and Trojans (Remote Access Tools - RATs) (CCEPL, 2024; Pospisil, 2020). Backdoor Installation this techniques attackers install backdoors that allow them to bypass normal authentication methods and regain access to the system (Naushad and Ajaz, 2022; Pospisil, 2020).Credential Harvesting this technique attackers are collecting and storing usernames and passwords to facilitate future logins.Rootkits, this is installing rootkits to hide malicious activities from detection tools and maintain control over the system.Creating User Accounts is done by Adding new user accounts with administrative privileges to ensure continued access. On the other hand, privilege escalation involves elevating user privileges on the compromised system. Cybercriminal seeks to gain higher-level access, such as administrative privileges, to control critical resources and systems (Surya et al., 2023, Naushad and Ajaz, 2022). Persistence Scripts which are scripts or scheduled tasks created by attackers to run at specific intervals on the compromised system (CCEPL, 2024; Surya et al., 2023). Attackers ensure that unauthorized access remains intact over an extended period, even if the initial entry point is discovered (Chandran, 2023).Trojans (Remote Access Tools - RATs) are malicious software programs used to create covert communication channels between the attacker and the compromised system (EC-Council, 2024). They enable remote control and data exfiltration (EC-Council, 2024; Naushad and Ajaz, 2022).

The common tools at this stage includes Cobalt Strike, Netcat, metasploit, Empire, Team viewer or AnyDesk, Poshc2, Rootkits and PowerSploit (Surya et al., 2023; Naushad and Ajaz, 2022). Cobalt Strike is a post-exploitation tool that allows attackers to maintain access through command and control (C2) channels, facilitating further attacks (Surya et al., 2023).Netcat is a versatile networking tool used to create backdoors and establish remote access to compromised systems (Surya et al., 2023). Metasploit offers various payloads and modules for creating persistent access through backdoors and exploits (Chandran, 2023; Pospisil, 2020).Empire is a post-exploitation framework that allows attackers to maintain access and perform additional tasks on compromised systems (Chandran, 2023). TeamViewer or AnyDesk are tools used by attackers to gain remote access to systems with legitimate remote desktop tools (Chandran, 2023; Pospisil, 2020). Poshc2 or "Posh Command and Control," is an open-source post-exploitation framework used in cybersecurity (Surya et al., 2023). It leverages PowerShell to maintain control over compromised windows systems, enabling cybercriminals to perform advanced post-exploitation tasks, such as lateral movement and privilege escalation, during security assessments (CCEPL, 2024; Surya et al., 2023; Naushad and Ajaz, 2022).

5.2. 6: Clearing Tracks Phase

Covering tracks refers to the various techniques and methods employed by cyber attackers to erase or obfuscate evidence of their unauthorized activities within a system or network (CCEPL, 2024; Surya et al., 2023). This stage is crucial for an attacker because it helps them avoid detection by security monitoring systems and forensic investigators, allowing them to maintain access and continue their malicious activities without being caught (Chandran, 2023). The purpose is to hide

the presence of malware, unauthorized access, or any actions taken during the attack, and to prevent system administrators and security teams from discovering the breach and mitigating it (Naushad and Ajaz, 2022). Clearing Tracks is a crucial step in cybercrime attack where cybercriminal, having completed their assessment, take measures to conceal any traces or evidence of their presence and activities on the target system or network (CCEPL, 2024;Naushad and Ajaz, 2022). This phase ensures that the penetration engagement remains covert and does not leave any lingering signs of intrusion, protecting the integrity and confidentiality of the assessment (CCEPL, 2024).

The common techniques used in stage are Log Deletion, Registry Cleanup, Anti-Forensic Techniques, Timestamp Manipulation, Rootkits, Obfuscation, and removing or altering Malware (EC-Council, 2024). Log Deletion is where criminals remove or manipulate log files that may contain records of their activities, ensuring that their actions go unnoticed (CCEPL, 2024; Surya et al., 2023). Registry Cleanup this a process of removing or changing entries related to the attacker's activities in the Windows Registry to erase any signs of intrusion (CCEPL, 2024). Anti-Forensic Techniques ate techniques to hinder forensic analysis, such as anti-forensic tools or encryption, are employed to make it harder for investigators to reconstruct events (Chandran, 2023; Pospisil, 2020).Timestamp Manipulation this technique used by attacker by changing the timestamps of files and logs to create the illusion that the malicious activity occurred at a different time or did not happen at all (Chandran, 2023). Rootkits, criminals install rootkits to hide processes, files, and system modifications from detection tools (Chandran, 2023; Pospisil, 2020). Obfuscation is the encrypting or altering code to make it difficult for antivirus software to recognize malware, and Removing or Altering Malware is done by cybercriminals after achieving their objectives, attacker may delete or modify the malware to obscure its presence (CCEPL, 2024; Surya et al., 2023).

The common tools that cybercriminal uses at this stage are LogClearing tools which specifically designed to delete or modify logs (e.g., LogCleaner) (Surya et al., 2023). Timestomp, this is a tool that manipulates file timestamps to cover tracks(CCEPL, 2024; Surya et al., 2023). Rootkits, e.g., Software like KBeast that hides the presence of malware and unauthorized access, and Obfuscation Tools such as ConfuserEx for .NET applications to make malicious code less detectable (EC-Council, 2024; Surya et al., 2023). Network Traffic Cleaning Tools (e.g., Scapy) which is the specialized tools like "Scapy" enable hackers to manipulate network traffic (Naushad and Ajaz, 2022). For instance, Scapy can forge or modify packet headers to obscure communication origins, making it hard for investigators to trace during assessments (Surya et al., 2023, Naushad and Ajaz, 2022). Registry Cleaning Tools which are Windows-specific applications are used to sanitize and modify the Windows Registry, eliminating or altering entries related to an cyber attacker's actions to prevent detection (Surya et al., 2023,Chandran, 2023). Anti-Forensic Suites is the comprehensive toolkits with various utilities designed to erase digital traces, modify metadata, and obstruct forensic investigations, preserving the hacker's anonymity and activities (CCEPL, 2024; Pospisil, 2020).

5.2.7. Exfiltration Phase

At this stage, the cybercriminal do exfiltration, which is the process by which an attacker retrieves sensitive data from a compromised system or network (Chandran, 2023). This stage is critical for attacker as it allows them to steal valuable information, such as personal data, financial records, intellectual property, or confidential business information (Surya et al., 2023). The purposeof exfiltration is to obtain sensitive data for malicious purposes, such as identity theft, fraud, corporate espionage, or selling information on dark web markets (CCEPL, 2024; Surya et al., 2023).Common

techniques are data compression, encryption, covert channels, and Remote Access Tools (RATs). Data Compression is the reducing of the size of data files to facilitate faster transfer (Surya et al., 2023). Encrypting data to protect it during transfer and evade detection by security systems.Covert Channels is a techniques that cybercriminalsare using unconventional methods to transmit data, such as steganography (hiding data within other files) or using DNS queries to leak small amounts of data (CCEPL, 2024). And, Remote Access Tools (RATs)which the criminals utilizing remote access software to transfer files directly from the compromised system to the attacker's system (CCEPL, 2024;Chandran, 2023).The common tools that are used by criminals at this stage are WinSCP which isa popular file transfer client that can be used for secure data transfer over SFTP, SCP, and FTP.Rclone is a command-line program to manage files on cloud storage, allowing attackers to upload stolen data to cloud services (Naushad and Ajaz, 2022). Other tools are FTP Clients which includes tools like FileZilla for transferring files using the FTP protocol.Steganography Tools that are Software like Steghide or OpenStego to hide data within images or other files (Surya et al., 2023). Moreover, PowerShell Scripts are custom scripts that can be used to automate the exfiltration of data in a stealthy manner (Surya et al., 2023).

5.2. 8. Impact Phase

This is last stage in the cybercriminal attacking. This is the stage refers to the actions taken by criminals after gaining access to a system, particularly those that result in significant damage or theft of data (Chandran,2023;Surya et al., 2023). The purpose of criminal at this stage is to achieve the cybercriminal's objectives, which may include stealing sensitive information, disrupting services, or harming the target organization (Surya et al., 2023). At this stage, the attacker can involve various malicious activities, including data theft, destruction, disruption, or even ransomware attacks (Surya et al., 2023). More specific, cybercriminal at this stage selling stolen data on the dark web, launching attacks (e.g., ransomware) and conducting further exploits based on the information gathered (Surya et al., 2023).The common techniques at this stages are Data theft, Ransomware Development, Denial of Service (DoS) Attacks, Destruction of data, Credential dumping, and Exploitation of further Vulnerabilities (CCEPL, 2024; Surya et al., 2023).Data Theft is theStealing sensitive information, such as personal data, financial records, or intellectual property. The appropriate tools are WinSCP for secure file transfers of stolen data, Rclone used to upload data to cloud storage and PowerShell scripts used to automate data extraction and transfer. Ransomware Deployment is also the techniques used by criminal at this stage. It is the encryption ofthe victim's files and demanding a ransom for decryption keys by using tools such as Maze and REvil. Maze is a ransomware variant that encrypts files and steals data to pressure victims and REvil is another ransomware-as-a-service (RaaS) that targets businesses for extortion (CCEPL, 2024; Surya et al., 2023). Another techniques is Denial of Service (DoS) Attacks, whichis the overloading a system or network to make it unavailable to users by using tools such as LOIC (Low Orbit Ion Cannon), and HOIC (High Orbit Ion Cannon). LOIC (Low Orbit Ion Cannon) is a tool used to perform DoS attacks by flooding a target with traffic and HOIC (High Orbit Ion Cannon) is similar to LOIC but offers more powerful capabilities (Surya et al., 2023).

Destruction of Data is techniques used by cybercriminal at this last stage of impact. Destruction of Data is the intentionally deleting or corrupting files to damage the target's operations by using tools such as Ccleaner and Custom scripts (CCEPL, 2024). Ccleaner is used to wipe files and logs and Custom scripts are scripts designed to delete critical files or databases (Surya et al., 2023).The Credential Dumping is the technique whichextracting credentials from compromised systems to

facilitate further attacks or lateral movement within a network by using Mimikatz and Windows Credential Editor (WCE) which is a powerful tool for dumping credentials from memory (CCEPL, 2024; Surya et al., 2023). Furthermore, the attacker at this stage may exploit further or additional vulnerabilities. This is done using common tools such Metasploit and Nessus (Surya et al., 2023). Metasploit which is a framework that can be used to identify and exploit vulnerabilities post-breach and Nessuswhich is used for scanning and identifying additional weaknesses in the environment (CCEPL, 2024). In addition, the study addressed the common tricks and determinants for each techniques and tools, and countering techniques on the 7 hacking stages. The aim is to help the investigators and other cybersecurity professionals to detect and prevent the cyber-attack in their organizations. The tricks are described for each stages of cyber-attack.

Table 1 shows the Modus Operandi (MO) of the cyber attacking stages. The table in column one described seven hacking stage or phases, which are reconnaissance, scanning, getting accesses, maintaining access, covering tracks, exfiltration and impact. In each stage, the techniques that applied by the cybercriminals are described in column two. These include Data theft, Ransomware deployment, Denial of service attacks, Port scanning, Vulnerability scanning, Data compression/encryption, and Covert channels for transfer, Deleting/modifying logs, Manipulating timestamps, Obfuscation techniques, etc. On the other hand, the tools commonly applied by cybercriminal described in column three includes Nmap, Maltego, WHOIS, Metasploit, Hydra, Social-Engineer Toolkit (SET), BleachBit, Timestomp, Custom scripts etc.

Table 1: Modus Operandi (MO) of the Cyber Attacking Stages

Stage	Objectives	Techniques	Tools	Psychological Tricks	Technical Tricks	Determinants	Protection Techniques
Reconnaissance	Gather information about the target	Open-source intelligence (OSINT), social engineering	Nmap, Maltego, Google Dorks	Curiosity, social proof	IP address enumeration, DNS queries	Availability of public data	Limit data exposure, privacy settings
Scanning	Identify live hosts, open ports, and services	Network scanning, vulnerability scanning	Nmap, Nessus, OpenVAS	Fear of unknown vulnerabilities	Service discovery, version detection	Network complexity	Regular vulnerability assessments
Gaining Access	Exploit vulnerabilities to gain entry	Exploit development, password cracking	Metasploit, Burp Suite, John the Ripper	Trust exploitation, urgency	SQL injection, buffer overflow attacks	System security measures	Strong passwords, patch management
Maintaining Access	Establish persistent access to the system	Rootkits, backdoors	Netcat, remote access Trojans (RATs)	Normalization of deviance	Creating scheduled tasks, modifying startup	System monitoring practices	Regular audits, endpoint protection
Covering Tracks	Erase evidence of the attack	Log manipulation, file deletion	CCleaner, custom scripts	Denial, minimizing consequences	Clearing logs, modifying timestamps	Logging practices	Comprehensive logging and monitoring
Exfiltration	Extract sensitive data from the target	Data theft, covert channels	PowerShell, FTP, HTTP/S, encryption tools	Justification, rationalization	Data compression, encryption	Value of data, data sensitivity	Data encryption, access controls
Impact	Cause damage or disrupt services	Denial of Service (DoS), destruction of data	LOIC, custom scripts	Fear, urgency	Overloading systems, data corruption	System redundancy	DDoS mitigation strategies, backups

Source: Developed from CCEPL (2024); Surya et al., (2023)and others

On the other hand, the table in column four describes the common tricks that are likely applied by the cybercriminals. These tricks which are deceptive tactics used to gain access or manipulate targets. These are Google dorking, social media profiling, Banner grabbing, OS fingerprinting, Pretexting, Phishing emails, Threatening victims with public exposure, Encrypting critical files, etc. In the two last column, column five and six column the table describes the determinants and countering techniques. These includes - Technical skill level Motivation (varies by goal) and Implement intrusion detection systems (IDS), regularly update and patch systems respectively.

6. Discussion

This study basically aimed to explore the cybercrime modus operandi. The study extracted and analysis several theoretical and empiricalacademic and professional studies and research articles, journals and policy papers. The study coined or extended the definition of the cybercrime modus to include the techniques, tools, psychological and technical tricks and their key determinant factors. The study defined the cybercrime operand *as the dynamic learned specific or unique means, characteristic, action or behavior possessed or shown by the cyber attacker in entering, executing, exiting and escaping from the crime scene; it involves all techniques, tools, psychological and technical tricks applied by cybercriminals before, during and after the cyber-attack*. This is mostly influenced by the time and technical changes. The term "learned" means the cybercriminals can learn through both informal and formal systems. The informal system includes the socialization with the criminal society or groups. That is, the criminal gaining criminality behavior or experiences through socialization with the criminal society (Turvey, 2013; Sundberg, 2020). On the other hand, the formal learning includes the procedural learning through official systems such as classroom learning in school and colleges.

This definition filled the gap of the traditional definition of the modus operand that was based only on the actions done at the scenes, that is during the commission of crime. The traditional definition was overlooked the two important aspects, that is, facts before the crime commission (planning scene), and facts after crime commission (exiting and escaping scene). In the modern or emerging crimes such cybercrimes and other organized crimes we must extended the meaning of the modus operand in order to understand the overall behavior, technical ability and skills of criminals. Therefore, we need a new definition of the modus operand that incorporate multiples features of the criminals skills and knowledge in use of the techniques, tools, psychological and technical tricks as the main components of the modus operand in the cybercrime. Thus, this definition, incorporated the action and behavior of the criminal done before, during and after the crime commission. This definitionprovided the significant contribution for both law enforcement and policy makers as it provides the comprehensive knowledgeable information of how the cybercriminals plan, organize, execute, exit and escaping from the crime scene.

On the other hand, the study provided the stages and targets of the cybercriminal attacking. The paper addressing eight (8) stages that the cyber attacking. This helps the law enforcement and other security professional to be aware on the cyber-attacks in each stage and then able to set appropriate preventing and combating strategies or plans at early stages. The study provided the aims, techniques, tools, psychological and technical skills on each stages of attacking and for each targets. This is usefulbecause the target, that is, individual or organizationstargeted with the cyber attackers will be able to understanding the aim or goals of the attacker, hence able toprovide the mitigation

strategies in their respective organizations.

In a specific way, the study closely examined both the psychological and technical tricks. The study found that the common psychological tricks are fear, urgency, trust, familiarity, authority, social proof and curiosity, emotional appeal. That is, the cybercriminals use these psychological tricks to deceive the end usersto provide their personal or confidential information or date to the cyber attacker, usual the phisherunknowingly. They are miming as the good men. The common means techniques of the cyber attacker is the phishing. The criminal create psychological phrases that tricks the individual to fear, or make of sense of urgency, or familiarity with the deceived issue or fact. These psychological trick phrases are created according to the target. For example, the common psychological trick phrases for individual target are“your account will be suspended in 24 hours unless you verify it." This message create a fear and sense of urgency to the receiver. That is, can lead the receiver to act on such instructions immediately. Moreover, the cyber attacker may craft the message such as"Hi [Your Name], we noticed unusual activity on your account." Or "Your account has been compromised! Click here to secure it immediately." These messagesdeceive the account owner to believe that the sender of this message he is familiar with the receiver. Then, the receiver can acton that instruction.
On the other hand, the cyber attacker may target the business entity by sending messages such "Dear Business Owner, immediate action is needed to verify your business account", or "Join thousands of businesses that have already updated their security," or “Only 5 items left! Order within the next hour for a discount!" These phrases are psychological tricks that traps or deceives the business owner to fear and creates the sense of urgency to act on the cyber attacker instructions. Once, the target action the deceived instruction of the cybercriminals, the target will be vulnerable for data theft or data loss.

Furthermore, the study explored the common technical skills that cybercriminal are using to phish or enter to the cybercrime commission. In realistic, the technical trick are usually targeted to trick or deceive the cybersecurityprofessionals, because they are crated to provide technical fake information. This deceived technical information are intendent to tricks or traps those who are knowledge on the cyberspace. This study highlighted some common technical tricks. The cybercriminals use tricks such as automated email generation for the hacking software or tools, alteration of email headers, spoofing of URLs, urgent requesting, manipulating DNS settings, using of unpatched software vulnerabilities, impersonating, overloading systems, SSL stripping, exploiting software vulnerabilities, payload delivery, system lockout and providing of input validation flaws.

Henceforth, the study provided the general and specific ways or techniques of countering the cyber-attack for each target. This is very useful because it provided the sense of awareness on the cybersecurity issue for the targets.The study suggested to some recommendations for end users to use spam filters, unsubscribe options, verifying sender authenticity, use SPF/DKIM, and get security training, anti-phishing tools. On the other hand, the study the application of HTTPS, secure DNS configurations, regular software updates, strong password policies, training the employees, verifying protocols, rate limiting and DDoS mitigation services. Moreover, the end user can use end-to-end encryption, secured Wi-Fi networks, installation of antivirus, keeps systems updated, perform regular system scans, regular backups, security software, regular code reviews, and security testing. Thesecyber-attackcountering strategies are established for each target to enable the targetto get precisionand specific action.

On the area that a researcher paid attention is to determine the *opportunistic factors* that leads the cybercriminals to commit crimes. That is, the determinants of cybercriminals. It is the very useful finding for both law enforcers and policy makers on the cybersecurity issues. This study examined several factors that determines the opportunity or likelihood of the cyber-attacks.These factors incudes the use poorly configured networks, user naivety, lack of awareness, vulnerable DNS servers, weak passwords, outdated systems, lack of security awareness, poorly secured infrastructure, insecure networks, weak encryption, insecure software, weak security practices, lack of backups and poor coding practices. Understanding the factors that determine the opportunity of the cyber attacker play a great role to study of cybersecurity to ensure the fair and secure uses of the cyberspace.

7. **Conclusion and recommendations**

The study aimed to introduce a new concept of interpreting and determining the modus operandi of the cybercriminals. That is, the modus operandi should be reflected to the whole or overall behavioral, technical and skills attributesof the cybercriminals. Moreover, the concept of modus operandi should be involve the all actions or behavior shown by the criminal in the whole process of the crime commission from preparatory stage to escaping stage, that is, at the entry, exit and exits and escaping In other words, the modus operandi in the cybercrime study should be involves the actions and behavior before,during and after the crime incident. Therefore, we define modus operandi as;-

"The dynamic learned specific or unique means, characteristic, action or behavior possessed or shown by the cyber attacker in entering, executing, exiting and escaping from the crime scene; it involves all techniques, tools, psychological and technical tricks applied by cybercriminals before, during and after the cyber-attack".

Therefore, the study suggested the investigations of the four crime scenes in cybercrime; *planning crime scene, execution crime scene, exit crime scene and escaping scene*. This means, that the cybercriminals most of them are well educated and skilled on ICT, and they use their knowledge and skills to commit crimes. In that sense, before to commit crime, they making decision or research on how (select methods, e.g. phishing) to enter the target, execute (selection of techniques and tools), exits (vulnerability) and escaping from the risk identified. Therefore, it is necessary the cybercrime investigator to understand the methods, techniques, tools and tricks those are used by the cybercriminals to enter, execute, exit and escaping.

On the other hand, the study highlighted the techniques, tools, trick, objective and determinants of the cybercriminals.Notably, in this paper we discussed the cybercrime modus operandi by encompasses the objective, techniques, tools, trick and the determinants of the cybercriminals. The study finding that the common and effective cyberattack tricks are psychological tricks such are fears, familiarity, urgency, trust, emotional appeal, curiosity. These psychological trick are crafted to short psychological phrases such as "your account will be suspended in 24 hours unless you verify it"; "Hi [Your Name], we noticed unusual activity on your account"; "your account has been compromised! Click here to secure it immediately", and others. These psychological phrases deceivethe users to act on their instruction in the sense of urgency, fear or familiarity. Therefore, from this finding we concluded that the most of the cyberattacks start with the phishing attacks which uses both psychological and technical tricks. Moreover, the psychological tricks are more

effectively than technical tricks.

Hence, the study recommended the application of protection or anti-psychological andanti-technical trick techniques such as uses of strong passwords, two factor authentication (2FA), antivirus, cybersecurity training, firewalls, incident response plans, employee training, security audits, threat intelligence, secure payment gateways, SSL/TLS, data encryption, Multi-factor authentication, cybersecurity awareness programs, strong cybersecurity policies and strong network segmentation.

References

Action Fraud. (2018). 419 emails and letters. Available at: https://www.actionfraud.police.uk/ a-z-of-fraud/ 419-emails-and-letters (Accessed: 04 November 2020).

Aransiola, J. O. and Asindemade, S. O. (2011) 'Understanding cybercrime perpetrators and the strategies they employ in Nigeria', Cyberpsychology, Behavior, and Social Networking, 14, pp. 759−763.

Ashworth, A. (2013). Principles of Criminal Law. Oxford University Press.

Baker, K. (2024). 12 Most Common Types of Cyberattacks. 2024 Global Threat Report, CrowdStrike, Australia.

Bates, S. (2017) 'Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors,' Feminist Criminology, 12(1), pp. 22−42.

Chandran, A. (2023). Ethical Hacking: 5 Phases, Techniques, and Tools. Medium, sept, 17, 2023.

Cobb, M. (2024).16 common types of cyberattacks and how to prevent them. TechTarget, New York, NY, 37 W 20th St. #904. New York, NY 1001

Dressler, J. (2015). Understanding Criminal Law. LexisNexis.

EC-Council, (2024). Certified Ethical Hacking; the 5 phases Every Hacker Must Follow, (505)341-3228. http://iclass.eccouncil.org

Fruhlinger, J. (2024). Logic bombs explained: Definition, examples, prevention. IDG Communications, Inc. 140 Kendrick Street, Building B, Needham, MA 02494, United States.

Global Initiative. (2024). 10 Biggest Cyber Crimes and Data Breaches to Date. Avenue de France 23 – Geneva, CH-1202 – Switzerland

GreyCampusEdutech Private Limited (CCEPL), (2024). Phases of Hacking. Aikya Vihar, Plot 218, B Block, Kavuri Hills Phase - II, Hyderabad – 500033.

Herring, J. (2018). Criminal Law: Text, Cases, and Materials. Oxford University Press.

Krebs, B. (2016). DDoS Attacks: What You Need to Know. Krebs on Security. Retrieved from Krebs on Security.

Krebs, B. (2020). "COVID-19 Fraud: How Scammers Are Taking Advantage." Krebs on Security.

Mali, P. (2024). Classification of Cyber Crimes. Lawyer Club India.

McAuliffe, C. (2017). Criminal Law: A Very Short Introduction. Oxford University Press.

McMillan, R. (2017). "Equifax Breach: What You Need to Know." Wall Street Journal. Retrieved from WSJ.

Naushad, D.R. and Ajaz, U.A.(2022). Ethical Hacking and Its phases. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 2(4), 23-26.

DOI: 10.48175/IJARSCT-3405
Pospisil, B. (2020). Modus Operandi in Cybercrime. Edith Huber, Gerald Quirchmayr, Walter Seboeck, |Pages: 17. DOI: 10.4018/978-1-5225-9715-5.ch013
ProofPoint. (2024). What is Email Spoofing? Proofpoint, Inc. 925 W Maude Avenue. Sunnyvale, CA 94085
Pudel, D. (2023). The 10 Worst Cyber Crimes Analysed. Skillcast, 80 Leadenhall St London, EC3A 3DH. United Kingdom.
Robinson, P. (2024). 15 Most Common Types of Cyber Attack and How to Prevent Them. United States, 600 Congress Avenue, 14th Floor Austin, Texas 78701
Samira Ibrahim, et. al. (2021). Types of Cybercrime and Approaches to Detection. IOSR Journal of Computer Engineering (IOSR-JCE), 23(5), 2021, pp. 24-26.
Simester, A. P., & Sullivan, G. R. (2016). Criminal Law: Theory and Doctrine. Hart Publishing.
Surya, B., Kumanan, T., Geetha, S. and Mehata, K. M. (2023). Tool for Hacking Phases. International Research Journal of Modernization in Engineering Technology and Science, 05(01), 1308-1317.
Symantec. (2000). ILOVEYOU Virus. Retrieved from Symantec.
Symantec. (2009). Understanding Trojans. Retrieved from Symantec.
TechBanz (2024). Cyber Crime Reasons and Prevention: Cyber Attacks. TechBanz, India.
Texas Tech University (TTU). (2024). Scams – Spam, Phishing, Spoofing and Pharming. Cybersecurity Awareness Program: Lubbock. TTU Office of the CIO, Lubbock, TX 79409
Wall, D. S. (2015). Cybercrime: A Multidisciplinary Approach. Cambridge University Press.
Ziegler, J. (2000). Salami Attack: The Case of the Missing Pennies." Journal of Cyber Security. Retrieved from Journal of Cyber Security.