Cyber Threat Intelligence

S M Nazmuz Sakib*

[1]S M Nazmuz Sakib (Orchid- https://orcid.org/0000-0001-9310-3014) (sakibpedia@gmail.com)*

[1] Graduate of BSc in Business Studies
School of Business And Trade
Pilatusstrasse 6003, 6003 Luzern, Switzerland

[1] Student of BSc in Civil Engineering
Faculty of Science and Engineering
Sonargaon University
147/I, Green Road, Panthapath, Dhaka

[1] Student of LLB(Hon's)
Faculty of Law
Dhaka International University
House # 4, Road # 1, Block - F, Dhaka 1213

[1] Student of BSc in Physiotherapy
Faculty of Medicine
University of Dhaka
Nilkhet Rd, Dhaka 1000

[1]Author Biography

S M Nazmuz Sakib is an eLearning expert and done more than 500 MOOCs or Massive Open Online Courses and experienced as an instructor in sites like Udemy. He has completed his BSc in Business Studies from School of Business And Trade, Switzerland with CGPA 4 in the scale of 4 and 97.06% grade marks on an average. He is also a certified Google IT Support Professional, Google Data Analytics Professional and IBM Customer Engagement Specialist Professional.

Abstract

The majority of the time, developing an intelligent technology entails obtaining data from a variety of sources. In most situations, the data acquired may be shared right away after it is collected, and it is based on the impact on present operations and operational requirements. Raw intelligence is based on little bits of information about occurrences and may contain doubts or

mistakes that must be rectified via reporting and analysis. Information is evaluated, contrasted, and weighted incomplete intelligence products so that conclusions may be drawn. Perfect intelligence, also known as completed intelligence, is the result of a series of events in the intelligence process. It double-checks a group of information or a single fact in order to reduce the risk of incorrect conclusions and deceit. Individuals, governments and organizations are always trying to find a way to remain secure from internal and external threat. None of the parties wants to lose crucial information or funds due to ransomware that has been explicitly discussed in this paper. The law formulates guidelines of collecting forensic information and data to prosecute cases of this caliber and they have been discussed in detail. There is software to help fortify network systems and while some of them are premium others are free and easily acquired over the internet. Knowing the cycles of threat intelligence is critical to the entire process and recommendations are offered to ensure organizations, individuals and countries remain safe from external and internal network threats.

Introduction And Background

Cybercrime is one of the most rapidly growing forms of criminal activity that continues to afflict the planet. They have evolved in their presentation forms, and they've had an impact on people's lives, businesses, military systems, and any other industry that relies on computer equipment or network coverage to function. Cybercrime is the act of gaining unauthorized access to a person's device and utilizing the information contained within for malevolent purposes. Credit card theft, identity theft, and cyber terrorism are among the offenses. The most serious form of cybercrime is cyber terrorism, in which the offenders frequently target a large portion of a community. The number of lives directly affected is frequently used to gauge the degree of the effect. Public utilities, such as utility lines, infrastructure, and communication networks, are

usually the major targets of cyber terrorism, which has a political objective (Reyns & Henson, 2016). If a country's defense system or automated transportation system were the major targets, the fallout would be terrible. Although no such attacks have occurred so far, the likelihood is great owing to global technology improvement. The methods employed to injure the aforementioned subjects are so varied that distinguishing them becomes a danger. The focus of this paper shall be ransomware because of its prevalence in major organizations and how it can be prevented through threat intelligence teams and software.

Security is a fundamental matter in all organizations for it to achieve goals and objectives. To ensure safety and access to an organization's data and information, specific measures and precautions are put in place. Some security threats affect the operation of organizations and make it risky for clients to trust them anymore (Butler, 2016). Some of the security threats include ransomware. Ransomware is a type of malware in which an IT expert accesses and encrypts the data files of an organization and demands a ransom amount of money in exchange for access to the organization. In this case, an individual has the authorization to access the files of an organization and no one else not even the authorized members of the organization, thus posing a threat. The cybercriminal uses the confidential data file as leverage to getting the amount they need. The cybercriminal threatens the victim organization or individuals to publish the information to the public. Therefore, the victim is forced or instead has no choice but to agree with the criminal terms to gain back access to their data. The payment transaction is done through forms of money and accounts that are untraceable even by the police.

The use of ransomware has grown dramatically in the past years, causing organizations and individual threats in security matters. Ransomware attacks may come through an email where the victim is tricked into the opening, thus giving access to the cybercriminals (Schmugar,

2018). By opening or downloading a trojan file, the victim is therefore not able to open the file anymore, and other confidential files are hacked too. To carry out the attack, the malware generates a specific key that encrypts the victim's data. The attacker provides the key and the procedure on how to pay the ransom to the victim as soon as the victim agrees to the terms. The victim sends the asymmetric ciphertext and e-money to the attacker. After receiving the payment then a symmetric key is sent to the victim. Using the final assigned key, the victim can decrypt the data and complete the attack, thus granting back access to the organization. The attacker's key is not exposed to anyone else, and only the attacker can use it in combination with the key sent to the victim to come up with the symmetric key to complete the attack. The assigned symmetric key only works for the specific victim (North, 2017). Ransomware attacks happen in many different ways. Malware can be in the form of an application attack where the attacker creates its shell to prevent it from opening. The attacker then demands a specific amount of money to remove the application shell and allow access. Until the ransom is made, the application does not open at all. Over time organizations have devised ways to minimize them through threat detection intelligence

Problem Statement

The hypothesis is the researcher's prediction regarding the outcome of the research where the relationship can be shown on the various variables. Involves collection and analysis of data that may either support or fail to support the solution to the research problem. The hypothesis show connection to the objectives of the study by providing a predicted answer. A hypothesis is a researcher's speculation on the outcome of the research by comparing the variables in the problem statement. The hypothesis of the study should be testable and realistic to provide answers to the research questions and objectives. The research hypothesis helps the researcher to

focus on proving that the statement of speculation is correct. The purpose of a research hypothesis is to help provide a comprehensive data collection on the problem statement in the research. From the objective section of a research project, one can quickly come up with a relevant hypothesis to the study. In this research on ransomware, the hypothesis will be derived from the objectives of conducting the research (Moore, 2016). The main aim of carrying the research on malware is to find out how it affects the operation of organizations. Using this objective, a hypothesis is derived, which is a ransomware attack that affects the process of the victim organization or individual.

Malware attacks threaten the internal security of organizations attacked. When cybercriminals attack organizations by encrypting their data files, it causes much threat to the guard with worries that more important and secret information may be exposed to the public. The attackers themselves pose a threat to the victims by forcing them to pay the needed ransom amount of money or just destroy the data without any provocation (Kirda, 2016). The information in the organization's devices such as computers is much vulnerable to malware attacks. The research hypothesis can be summarized as follows:

- Malware attack affects the operation of the victim organization or individual.
- Malware attacks cause a threat to both the internal and external security of an organization.
- Organizations devices such as computers are much vulnerable to malware attacks.
- Malware ware attacks can be prevented
- The ransomware attack methods are sophisticated, and only the attacker provides a key for data decryption.

Literature Review

The process of acquiring, collating, analyzing, integrating, evaluating, and interpreting data yield intelligence. It's a tailored information product that gives an adversary or the US the information it needs to advance its national interests. One of the most important tasks of intelligence is the reduction of the complexity inherent in the observation of external actions. The most obvious use is that hostile intelligence agencies might seek information about military capabilities or other things that directly attack US national security. Different organizations or hostile nations may try to dig in in other circumstances information about economic programs, proprietary information from private U. S corporations, or U.S. diplomatic negotiating positions. In most cases, the information under attack may give an enemy a clue that might enable him or her to adopt a well-thought-out strategy to attain his or her goals.

Vulnerability Assessment

Ransomware is a form of malware that has brought significant threats to organizations and individuals and states in the past ten years. Its attacks had significantly increased as compared to ancient times when technology was not much appreciated and developed. Organizations and individual victims are at risk of losing their confidential information and also encountering a financial loss after the ransom payment (Kirda, 2016). It is very risky for an organization's operations since the amount of money demanded by the attackers is usually a lot, thus affecting the financial sector of the business, which may lead to closure. Security measures can help prevent attacks by ransomware and minimize the risk to the victim organization (Sinha, Pullat, Pradhan, Lancioni, Rajan, Cochin & Schmugar, 2018). Every organization and individual using electronic devices such as cell phones and computers to store their information is faced with the threat of attacks by ransomware. The increased ransomware attacks prove that most organizations need to secure their data files to prevent frequent and desired attacks. The

vulnerability of an organization or individual to ransomware attacks can be determined by assessing its security hygiene and measure.

For organizations to stop the attacks by malware infections, they need to ensure that the right and adequate security measures are in place. Organizations need to have clear visibility and access to all points in their network systems (Kirda, 2016). An update of the network systems is essential and needs to be carried out frequently to ensure the safety of all the data files in the organization. It may be difficult for an organization to be able to keep track of all up-to-date status of the network systems (Scaife, Carter, Traynor & Butler, 2016). Even though it is challenging to keep track of all the endpoints up to date status, security attacks can be reduced by ensuring that the endpoints where crucial data files are stored are safe and not vulnerable to ransomware. By using centrally collecting vulnerability scan data sources in computer devices, organizations and individuals can be able to identify the endpoints in their network which are vulnerable to ransomware and take action. Vulnerability scanners are used by organizations and individuals to assess the vulnerability of their data files.

Vulnerability scanners help organizations to be able to see which endpoints in their network systems have many risks to attacks as a result of ransomware. Appropriate measures to stop such vulnerabilities are put in place. A procedure is used to select the most relevant data file and assess their vulnerability (Egele, 2017). A report is built to allow access and visibility to the endpoints in the network system which are vulnerable to any computer virus such as malware and ransomware. Vulnerability assessment is done to ensure that there is security to data files in an organization and help to stop and prevent security threats due to any malware form from occurring. By gaining visibility to all network system endpoints and vulnerability environments, then an organization can come up with mitigation procedures that help stop ransomware attacks

from happening. Vulnerability assessment is essential in managing the security of organizations. Though it is challenging to keep track of every up-to-date status of all system endpoints, it is essential to ensure the safety of all the data files from malware threats.

When it comes to cyber terrorism, gathering, evaluating, storing, authenticating, and translating threats to accessible information becomes a more difficult task when the forensic team doesn't know the exact target and method of execution. Before beginning their search, the forensic team must be aware of the degree of the damage as well as the negative consequences. This simplifies the work by saving time and money for both the monitored individual or corporation and the threat intelligence team. Before the forensic team is tasked with determining the actual degree of the damage, the person or people being investigated should explain whether or not the information should be utilized as evidence.

Strategic and operational intelligence are the two types of intelligence. Operational intelligence specializes in present or near-term occurrences. It is utilized on a continual basis to evaluate the anticipated and present ability of an operation or program, but it does not end in long-term predictions. The majority of intelligence efforts help to produce operational intelligence. Strategic intelligence provides policymakers with the data they need to make long-term choices and formulate national strategies. It generally evolves through time, with the impacts being estimated and intelligence studies being produced.

The Cycle of Intelligence

This is the method for obtaining, producing, and sharing intelligence so that it may be used by people. The Intelligence Community in America follows a five-step procedure, however other countries could also use a unique identifier for it. Planning and direction, collection, analysis, and processing, production, and distribution are the phases in the intelligence cycle.

Planning and Guidance

This is the initial phase in the process, and it entails overseeing the overall intelligence endeavor, which involves selecting a requirement for a need for information to the delivery of the intelligence product to the consumer. Identifying, evaluating intelligence needs, issuing information collection requests, prioritizing, developing collection plans, converting specifications into observables, distribution, production, and continually monitoring whether the gathered data is available are all part of the process. Specific collection capabilities are determined in this initial stage based on the type of data required, the presence of gathering assets, and the vulnerability of the targeted action to various types of collecting activity.

Collection

This is the second stage, which entails gathering information and distributing it to production and distribution elements. It also entails establishing collecting procedures that assure the utilization of intelligence resources. Intelligence gathering requirements are created to meet the demands of future customers, and they are given specific responsibilities to collect data. These are difficult jobs that may necessitate the utilization of a variety of intelligence disciplines for data collecting. Task redundancy can help prevent the breakdown or loss of a collecting asset. It guarantees that if a collecting asset fails, it is balanced by alternate or duplicate assets that may meet the collection demand. The employment of several types of collection systems contributes to redundancy. It also allows for the gathering of various types of data that may be used to contradict or validate possible evaluations. To facilitate data sharing and give chances for tip-off exchanges across assets and cross-cueing of assets, collection operations rely on quick, secure, reliable, and robust communication. Following the collection of data, it is correlated and transmitted for processing and production.

Processing

This is the third stage, and it is the modification of gathered data that is ideal for intelligence creation. Here, incoming data is converted into forms that intelligence analysts may freely utilize in the production of intelligence. Intercepted messages may be reduced to textual form for comprehensive analysis, translation, and comparison with other data during processing. Photographic processing, video creation, and the correlation of data acquired by technological intelligence platforms are examples of other sorts of processing.

Production

Analyzing, assessing, interpreting, and incorporating raw information and data into completed intelligence products for expected or known objectives and applications is the fourth stage. The product might be made up of many source databases and collections or a specific source database and collection. The demands of the customer must be at the forefront of intelligence development to be effective. It should be accurate, timely, and objective. The analyst must exclude everything that is irrelevant, incorrect, or unnecessary to the intelligence need. The analyst can use the diagnostic effort to identify extra collection operations that are needed to fill in gaps left by prior or existing collection intelligence databases. The final intelligence product must give the user a grasp of the topic area and allow them to form analytical conclusions based on the facts supplied.

Dissemination

This is the final phase, and it involves delivering intelligence to the user in a usable format. Consumers can get intelligence in a variety of ways, including images, vocal reports, written reports, and intelligence databases. Interconnected data and communication networks, as well as physical exchanges, can be used to disseminate information. For three main reasons, the OPSEC program manager should be familiar with the intelligence cycle. The first one is that

knowing this information enables them to devise countermeasures to counteract the adversary's gathering efforts. The OPSEC project coordinator can assess if his program, facility, or operation is likely to be targeted because of opponent intelligence plans gleaned through US intelligence collection. Knowing an adversary's patterns and collecting methods helps him or her to devise effective countermeasures that conceal or change indications. The second reason is that it allows the manager to take part in the information gathering that is needed to support his OPSEC program. The administrator should be aware of the many risks that endanger his program; otherwise, he or she will be unable to take measures to prevent the adversary from accessing data that might include confidential information. It also allows him to figure out how to get the intelligence he needs to carry out the OPSEC process. Finally, knowing the analytical preferences of the opponent may be utilized to create deception algorithms that fool the adversary by confirming false views.

Methodology

Disciplines of Intelligence Gathering

Adversaries employ the majority of intelligence disciplines to gather information on the United States. Signal intelligence (SIGINT), human intelligence (HUMINT), open-source intelligence (OSINT), imaging intelligence (IMINT), and measurements and signatures intelligence are some of these fields (MASINT). To some extent, enemies utilize each of the disciplines against the United States. Most governments, as well as many subnational and commercial entities, have HUMINT capabilities that they use to gather data on their competitors and their adversaries. Because the American society is not discrete, open-source intelligence is successful in targeting the United States. Professional and technical magazines are frequently extensive sources of information on US economic and government operations. The growing number of online databases has increased rivals' and enemies' ability to build personalized digital solutions on industrial operations and the United States by enabling analysts to revisit enormous amounts of data in a short period of time. As more information becomes available online, open-source collecting becomes a danger. This is a threat that OPSEC program managers should be aware of in order to ensure that safety measures are used to stop exposure of the program of activities through data publication in public media. Information may be collected via SIGINT, MASINT, and IMINT by intelligence-gathering agencies. The intelligence organization's technological skills generally put these collecting capacities at a disadvantage. In comparison to the two collecting capacities, MASINT is employed by a small number of countries.

HUMINT

The majority of human intellect is generated from human sources. Overt collectors, such as military attachés and diplomats, are generally the ones that gather HUMINT. It's a time-honored way of gathering intelligence about a hostile adversary. HUMINT refers to activities that are sensitive, overt, or covert, as well as the people who support, oversee, monitor, and

utilize them. Members of official delegations, military attachés, debriefers at refugee centers, and diplomatic staff are all examples of overt HUMINT analysts. Exploiting conference materials, unclassified publications, and congressional hearings are examples of overt HUMINT efforts. running interrogation facilities for war prisoners and refugees, as well as debriefing lawful visitors who traveled to nations of interest to a country's intelligence service. There are accords that allow for the use of technological collecting capabilities to determine national declarations and the on-site are defined. The treaties are the Strategic Arms Reduction Treaty (START), the Conventional Forces in Europe Treaty (CFE), and the Nuclear Nonproliferation Treaty (NPT) Intermediate-Range Nuclear Forces (INF), Bilateral Agreement between the United States and Russia on Chemical Weapons. Additionally, Open Skies Treaty (OS), Threshold Test Ban Treaty (TTBT), and the Peaceful Nuclear Explosions Treaty (PNET) usually enable information to be gathered from installations that are sensitive even though on-site inspections are allowed. HUMINT can allow access to the compartmented information and internal memoranda. It saves on the cost compared to collection systems that are technical. It may also provide evidence such as copies of diplomatic or policy documents, the blueprint of facilities, or adversary plans.

SIGINT

Electronic intelligence (ELINT), communications intelligence (COMINT), and foreign instrumentation signals intelligence are all types of signals intelligence (FISINT). Non-communications broadcasts, such as radar, are analyzed and intercepted as part of ELINT. It's used to determine an emitter's position, identify its properties, and infer the properties of supported systems. COMINT can be acquired through fiber optics, radio waves, or any other medium of transmission. FISINT is the collection of telemetry from an adversary's weapons systems as they are being tested. Transmissions from terrestrial facilities and communications satellites can be inspected by SIGINT facilities.

MASINT

This information is produced from a qualitative and quantitative examination of data collected from technological sensors in order to identify any characteristics associated with the sender or source emitter. This data is then utilized to assist with the measurement of similar equipment. Infrared intelligence (IRINT), nuclear intelligence (NUCINT), and radar intelligence are examples of MASINT disciplines (RADNT). MASINT identifies information patterns that have not been tampered with by sensors since it works in various areas of the electromagnetic spectrum. There are no safeguards in place to preserve the signatures.

IMINT

It's a result of imaging analysis, and it comprises optically reproduced things on film, electronically, on electronic display devices, or on other media. Radar sensors, visual photography, electro-optics, and lasers can all be used to create imagery. The use of data to classify, locate, and recognize things or organizations is referred to as IMINT. It may also be printed on both soft and hard copies. Imaging is important because it allows activities to be watched, it offers geolocation prediction accuracy for weapons system targeting, and it can be utilized by imagery sensors to map regions of critical value across broad areas. The disadvantages of imagery are that it requires a technologically oriented infrastructure, imagery quality is usually affected by weather and darkness.

OSINT

Open-source intelligence is the usage of materials available to the public and adversaries and other intelligence agencies. Open-source information saves time and is the only information that is available in the event of an emergency or a crisis. It is also used to obtain trade secrets or classified data. It can also be used to offer information on technical processes, organizational dynamics, and research activities not available in other forms. The disadvantages are that the

press can be used as a means of deception and that articles in scientific journals or military journals usually represent a desired rather than actual capability.

All Source Intelligence

This involves all the information sourced through IMINT, OSINT, SIGINT, HUMINT, and MASINT. The aim of such of effort is to form comprehensive information and to use many sources to obtain key points of data. The advantage of all these sources of intelligence is that it enables comprehension of its operation and it can be the most dangerous threat to an OPSEC manager but luckily, only a few nations can be able to achieve these efforts.

Results

Various forensic tools may be used to do all of the searching, gathering, analyzing, authenticating activities, and storing depending on the nature of the assault and the tactics employed by the perpetrators. Spyware, spoofing, worms, Trojan horses, infections, phishing, adware, hacking, and pings are some of the ways that attackers can utilize. As previously stated, the investigation team should be aware of the particular type of assault, the devices, people, or data that were targeted, and the amount of the damage (Kondiles et al., 2018). This may aid in the minimization of future threat-related damages as well as resources. The type of intrusion, management, prevention, and recovery systems that the investigated element had before the attack should also be surrendered so that the precise breaches and sites of infiltration that resulted in threat issuance of information loss may be identified. Regardless of the size of the technological equipment or the number of network connections that exist, they should all be turned over to the forensic team for an appropriate examination. Depending on the gravity of the situation and the party that requested the threat intelligence information, the search must always

adhere to the law, and it is recommended that the crime be reported to the authorities. Reporting the incident is a commendable decision because it will aid authorities in apprehending the criminal and preventing a repeat attack on the same or a different target. If the case being investigated is a data breach, the courts may grant the threat intelligence team a search warrant on the suspect, which could speed up the investigation and information recovery procedure.

Digital forensic tools and electronic discovery tools are the most common instruments used in forensic audits. Electronic discovery tools are sometimes known as e-discovery tools. These two tools are used independently with their collection of software packages, or they can be combined to form a single tool. Although the tools are nearly the same, forensic tools can be enlarged to undertake articulate audits or contracted to refine the search (Jaferian et al., 2014). Since forensic tools are a form of e-discovery, they are far more superior. E-discovery tools can be replaced with forensic tools, however, the latter cannot fulfill the same functions. This is dependent on the number of devices and networks to be examined, the number of people participating, and the period in which all of the activities must be completed. Regardless of the technology used, all methods must adhere to the law's evidence collection criteria. The data must be kept in a proper chain of custody and it should not be manipulated or destroyed since it may be used as evidence in a court of law. If the data is deleted or manipulated in any way that prevents it from being processed into information, it will be impossible to defend in court, and the entire procedure will be a waste of time. There are a range of forensic tools available from vendors, some of which can be tailored to match the element's demands, and the team should be informed if the element under investigation has subscribed to either of them before the evaluation process begins.

The tools should have the following functions, regardless of the acquisition: acquisition or archiving, search or assessment, and reporting. The following competencies must flow smoothly and in a systematic manner. The forensic team can choose whether or not the capabilities are automatic or require mechanical stimulation. The tool should be able to copy most of the data as it was in operation during the operation of devices, software, networks, program, and storage devices as they were during the attack. After that, the duplicate or duplicates must be compared to the original parts that were given to the team of investigators before the investigation began. The search feature makes the job easier for forensic auditors by allowing them to look for keywords in the papers they're looking at. A powerful search feature can evaluate and key phrases from emails, encrypted files, erased data, network protocols, temporary files, hidden content, and secured networks, among other sources (Jaferian et al., 2014). This feature saves a lot of time. The tool's reporting feature allows it to generate a complete report that includes all of the audit records. This phase establishes that the audit was carried out per the law and that none of the parties' rights were infringed upon. Because it has most of the above functionalities and can be scaled up or down depending on the devices and networks to be covered, I propose EnCase Forensic software. However, depending on the task at hand, there are quite a variety of instruments that can be employed, and many forensic professionals prefer to use most of them so that no information is missed.

The Five Phases of The Threat Intelligence Lifecycle

The threat intelligence lifecycle encompasses cybersecurity programs, fraud, and physical operations. The five phases of the threat intelligence lifecycle transform raw data into finished intelligence. The objectives at each phase are planning and collection, direction, analysis, dissemination, production, and feedback.

PHASE 1: Planning and Direction

This is the most essential because it sets the pace for which all intelligence activities. It highlights the tasks and goals for the threat intelligence program which is referred to as intelligence requirements. (IRs). IRs should also spell out the objectives of the team and values the finished intelligence will present. The Chief Information Security Officer usually directs the planning at this stage.

PHASE 2. Collection and Processing

At this stage, the quantity and quality of data are essential. Intelligence collection usually forms the scope of the sources including threat types such as compromised credentials, phishing, network logs, malware, leaked variants, and common vulnerabilities and exploit (CVEs). Processing seeks to structure, normalize and deduplicate all of the collected data. Specific processing procedures include translating conversations derived from a foreign language, dark web marketplaces, and forums, lowering the volume of raw data, and metadata extraction from malware samples.

PHASE 3. Analysis

This is a human-oriented process and its aim is to contextualize processed threat intelligence through the application of the known structural data or advanced correlation and data modeling. With the development of artificial intelligence and machine learning, the processes will become automated. This enables the staff to focus more on investigations and strategic tasks.

PHASE 4: Production

This step focuses on organizing finished intelligence into easy-to-digest graphical charts, reports, and dashboards. It is crucial to obtain the most important information and draw conclusions from the data and analysis completed in the earlier phase. Appropriate courses of action will include prepared decision trees and procedures to initiate threat remediation, patch

management, and incident and ransomware response. Production stakeholders work on reports and prepare the communications to key decision-makers and final team members. The final audience of the finished threat intelligence has the authority to assess the analysis and decide whether or not to take action.

PHASE 5: Dissemination and Feedback

This is important in order to derive results and attend to the risks and fraud. The teams responsible for strategic planning and resource planning are vulnerability management, security operations (SecOps), senior leadership, and third-party risk. Stakeholders upon receiving the finished intelligence, review the findings, form key decisions and give feedback to continuously refine intelligence operations. Improvements in this phase tend to gravitate towards the time to reach the final delivery, efficiency of intelligence activities, and speed.

Recommendations

Due to the increasing cases of malware attacks in the past years, organizations and individuals need to come up with strategies and techniques that will help prevent the attacks from happening. The malware prevention methods can be divided into three forms which are end-user security methods, network, and system security, and finally responding to the attacks (Brewer, 2016). The following are some of the network and system security measures to prevent malware attacks; backup systems help to prevent malware attacks since the availability of the secured backup files makes it possible to access the data files even after a malware threat. Also, though there is a backup system for the organization's data, routine testing is needed in case of an infection by the malware. For better operations for the organization, it is essential to ensure security to the backup systems.

Antivirus and antispam programs are one of the most effective methods to prevent malware attacks and threats. Organizations should do regular check up on the systems and networks to ensure there are no areas of malware vulnerability. Antivirus scanning detects and identifies areas of malware vulnerability, and by automatically updating data signatures, security is guaranteed (Maggi, 2015). Antispam systems and warning banners also help prevent malware attacks from occurring. The antispam program stops compromised emails from going through to the system. With the help of warning banners, a warning is made for emails and links sent from unknown sources, therefore, alerting the organization or individual not to open or access them (Kharaz, Arshad, Mulliner, Robertson & Kirda, 2016). Other malware prevention methods include; restricting internet access, keeping all networks and systems updated, and using office viewer software to open files from the email instead of the full office suite which is more vulnerable to malware threats (Andronio, Zanero & Maggi, 2015). It is also essential to secure the end user by ensuring that all users close their browsers after use. Finally, responding to the attack and paying the demanded malware is a prevention method to avoid more risks such as losing the crucial data files completely.

Because it has most of the above functionalities and can be scaled up or down depending on the networks and devices to be covered, I propose EnCase Forensic software. However, depending on the task at hand, there are quite a variety of instruments that can be employed, and many forensic professionals prefer to use most of them so that no information is missed. To make a complete evaluation package, add e-discovery tools, slide-window programs, and survey tools to the forensic tools. E-discovery technologies are designed to extend the scope of the investigation and allow the team to cover a lot of territory in a short amount of time. Intrusion detection systems, log analyzers, network analyzers, and web proxy reporters all use survey tools

to monitor activities that exceed the pre-configured threshold on intrusion detection systems, traffic, log analyzers, web proxy reporters, and network analyzers. Slide-window software keeps track of how systems behave over time. The first step in the process is for the investigation team to have certain goals in mind. The finest investigation tools must be capable of working over such a network, allowing them to work on networks and devices that are isolated or compressed.

This type of tool will reduce the amount of groundwork required, and all operations can be completed by a small group of experts in a smaller space. Another benefit is that the forensic task was to be completed within a specific timeline will be reduced greatly (Kondiles et al., 2018). Ordinary forensic audits using manual forensic tools could go to five months, but network-based methods can be completed in as little as three days. The problem of whether the forensic team will subcontract the expertise or create in-house forensic software goes unanswered. Although the former appears to be the ideal option because the service can be disposed of and has no long-term financial responsibilities, the latter is indeed the best alternative. In-built solutions are typically customized and should be coupled with other systems that are automated to enhance the efficiency and output of a company's entire information technology infrastructure. while small organizations may opt not to acquire such services and software, large corporations should have them for their security. The admissibility of the obtained data in a legal proceeding is another element to consider. The cybercrime act has numerous regulations that govern how forensic audits should be conducted. The evidence must have been acquired legally, as within any other matter before the judge, and neither party should argue that their rights were abused. This means that all of the information gathered must be subject to a search warrant.

A search scientist will also have to design all of its criteria before the request is made because of the intricate nature of Information Technology. It should state the type of items it seeks as well as the exact position of the device, zip file, or folder that has the needed information. If the team takes a broad approach to the problem, it can be a torturous process. A warrant can be denied due to a lack of clarity, and overreaching the legal border can lead to the evidence being revoked by the jury (Reyns & Henson, 2016). After the full investigation is completed and the damage extent determined, the person or entity should stud his system or infrastructure to protect the event from happening again. This can be accomplished by changing systems passwords and upgrading security for all devices and accounts that access a database.

Conclusion

From the above discussion, it is clear to conclude that organizations and individuals are vulnerable to every type of malware including ransomware attacks through computer devices they use. The ransomware attacks pose a threat to the security of the victim and risk in their finances (Maggi, 2015). The operation of an organization is affected by ransomware attacks. Ransomware is a very risky form of malware where crucial data files of an organization are put at the threat of been exposed. Most of the intrusions occur because organizations choose to ignore network safety protocols and refrain from acquiring the latest safety software thereby risking their operations being grounded. Therefore, it is essential for security measures that will help prevent malware threats and risks to be put in place in organizations for safe operations. Most of the information can be found online and the products and services can be outsourced if there are no internal forensic and threat intelligence teams.

References

Andronio, N., Zanero, S., & Maggi, F. (2015, November). Heldroid: Dissecting and detecting mobile ransomware. In International Symposium on Recent Advances in Intrusion Detection (pp. 382-404). Springer, Cham.

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. Network Security, 2016(9), 5-9.

Jaferian, P., Hawkey, K., Sotirakopoulos, A., Velez-Rojas, M., & Beznosov, K. (2014). Heuristics for evaluating IT security management tools. *Human–Computer Interaction*, *29*(4), 311-350

Kharaz, A., Arshad, S., Mulliner, C., Robertson, W., & Kirda, E. (2016). {UNVEIL}: A Large-Scale, Automated Approach to Detecting Ransomware. In 25th {USENIX} Security Symposium ({USENIX} Security 16) (pp. 757-772).

Kondiles, G., Starr, R. C., & Jablonski, J. (2018). *U.S. Patent Application No. 15/722,900*.

Moore, C. (2016, August). Detecting ransomware with honeypot techniques. In 2016 Cybersecurity and Cyberforensics Conference (CCC) (pp. 77-81). IEEE.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International journal of offender therapy and comparative criminology*, *60*(10), 1119-1139.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016, June). Cryptolock (and drop it): stopping ransomware attacks on user data. In 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS) (pp. 303-312). IEEE.

Sinha, B., Pullat, A. C., Pradhan, A., Lancioni, G., Rajan, P. R., Cochin, C., & Schmugar, C. (2018). U.S. Patent Application No. 15/392,848.