International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 653-657 www.ijaem.net ISSN: 2395-5252

Key Infrastructure Security and Data Warfare

Dr. Alex Mathew
Dept. of Cybersecurity Bethany College USA

Submitted: 10-03-2022 Revised: 21-03-2022 Accepted: 23-03-2022

ABSTRACT— In the last few years, technological improvement and digital transformation have led to various types of cybercrimes. Cyber-attack has been a big issue in America. The government of the United States has been at the forefront to tackle the issue of cyber-attack that is now a national thereat. Due to low investment in this sector, there are no resources to counter sophisticated cyber-attacks. However, thanks to digital forensics in countering cyberattacks fostering cybersecurity. Lost data can be traced whether deleted or from a suspect's device. Digital forensic uses artificial intelligence, and machine learning to aid in digital investigations together with Internet of things forensics, cloud forensics, and social media forensics. The digital systems should be hardened further and be monitored always for intrusion.

Keywords— Cybercrime, cybersecurity, Digital Forensics, data warfare, Artifical Intelligence

I. INTRODUCTION

With the evolving technology, the world is now driven by digital technology and social networks. With the growing digital transformation, cyber-attacks are becoming a threat to the digital world-leading to privacy infringement, loss of revenue as well as reputation [1]. In the United States (U.S.), cyber-attacks have become an issue not only to individual organizations but to the government as well. Cyber-criminals normally focus on critical infrastructure. Some of these sectors cannot fight against cybercriminals. There are huge investments in this sector and an attack becomes a big issue. Even with the advancement in digital forensics, criminals have increased cyberattacks with high technology hence able to penetrate even in controlled environments. With advances in digital forensics, cybercriminals have further developed anti-forensic techniques [2]. With these, forensics also face new challenges of cyber threats and malware every other time. Responding to cyber-attack needs a credible forensic approach. In this study, cyber threats will be identified and the most relevant digital forensic response to improve cybersecurity on such incidents.

The proposed methodology in this study will review journal articles together with literature materials that have information on cyberattacks and forensics so as to draw favorable conclusions. The study will show machine learning, deep learning, and artificial intelligence tools used in forensic investigation with various modules and functions [3]. The block diagram in fig. 2 is divided into three phases that are threat identification, vulnerability, and forensic approach [4]. First cyber-security threats will be identified then later the recent forensics that are being used to counter cyber-attacks.

Cybercriminals commit different crimes including hacking, cyberbullying, spamming, phishing, and blackmail [5]. One cyberattack against some critical sector can have a huge impact on the global society and economy hence can be used as a weapon of mass destruction (WMD [6]. For instance, in 2015, an attack in Ukraine associated with a cyber-attack by Russia caused a power outage in some of the power distribution companies in the country leaving thousands of people without power for six hours in the middle of winter all in the name of gathering information on company operations in the central and regional facilities. With similar and related kinds of cyber-attack threats, a nation faces military threats.

Cyberattacks take different forms and progress as they intensify. Cyber gangs use different attack strategies in a single attack. Cybercriminals can steal user data or credentials such as login details and credit card numbers or use ransomware hack [5]. They also use malware and structured query language (SQL) among others. The SQL attack inserts some codes into the server's SQL database software that reveal data not available from a webpage. If the user does not have good cyber practice and the system is vulnerable this cyber-attack may persist and combined with malware can develop further disruption strategies. The ransomware hack attacks

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 653-657 www.ijaem.net ISSN: 2395-5252

critical infrastructure gaining control of the systems by inserting malware into the system causing a denial of service (DoS) [7][8][9]. With a ransomware attack, the operation of the organization is halted until payment is known as "protection payment" to the attackers is made for the company to regain access to the systems. Some companies such as the colonial pipeline and JBS USA have been victims of ransomware attack.

Cyber-attack takes place in steps. The first step is reconnoitering, whereby the attacker collects information about the victim [5]. After gathering information, using proxies, virtual private networks (VPNs), or the onion router (TOR), an attack can be made either from the inside or outside, by a direct or indirect human interaction. Then the information is disclosed using criminal software installed in the system that reveals the business secrets or steal. Information is then transferred through copying without detection. Data is then retrieved quickly without detection, silently, or by diverting attention to another scene. Cyber-attackers cannot be identified easily because they are anonymous. They can only be classified depending on the type of crime, attackers' intentions, knowledge, and skills, as well as the available resources and manpower.

II. PROPOSED METHODOLOGY

Figure 1

Cyber Crime Flowchart

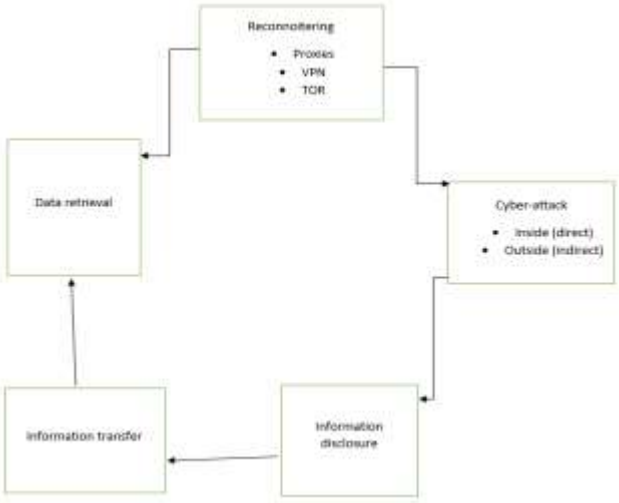
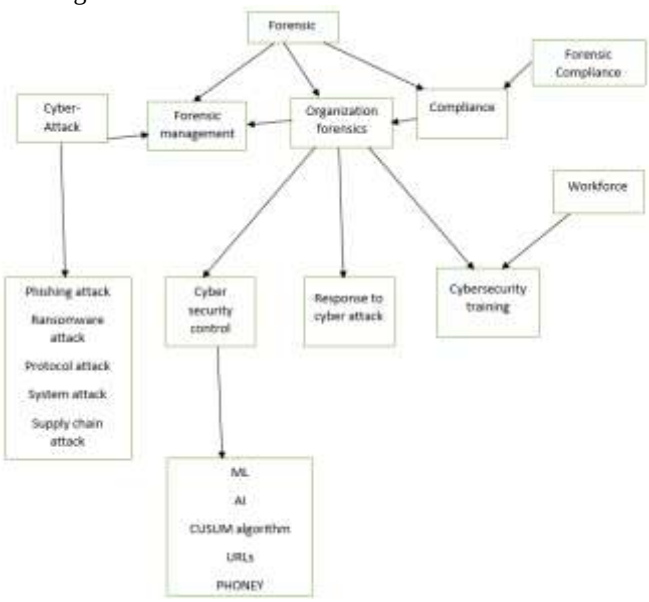


Figure 2

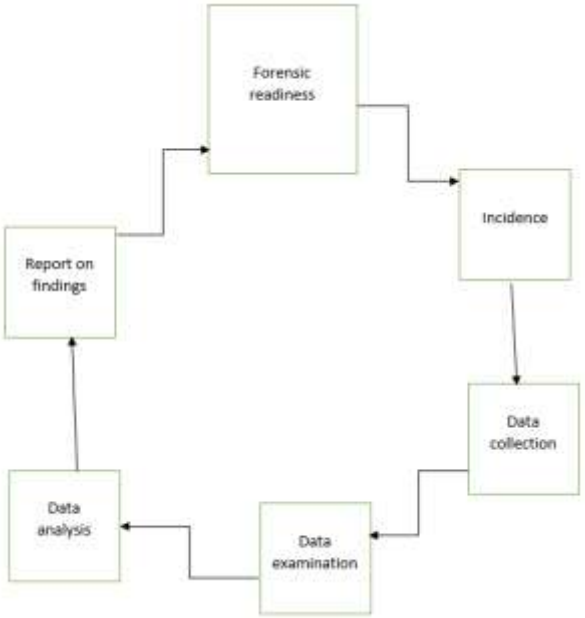
Cyberattack Forensics Block Diagram



International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 653-657 www.ijaem.net ISSN: 2395-5252

Figure 3

Forensics Cycle



As the cyber-crimes started to increase in the 90s, digital forensics developed to respond to digital investigations and crimes [10]. Forensics helps investigate several kinds of cyber criminality such as DoS, website high-jacking, virus, and ransomware attack among others [9]. Organizations should take a tall to protect themselves from a cyberattack no matter the policies put in place by the government against cyberattack [7]. With the current trends and reactions to cybersecurity, cyber-attacks are likely to continue. Therefore cybersecurity responsibility should not only fall on the government but individual organizations should protect themselves against growing threat.

Some organizations have chosen to merge information technology [IT] systems with operation technology (OT) systems for control in case one of the systems was attacked. Cloud computing, social media, and the internet of things (IoT) are used in forensics [11] [8]. In cloud computing, scientific principles are used to collect data and reconstruct events using data encryption [12]. Social media forensics is used when posts on Facebook, Instagram, and Twitter among others are used for investigation [13]. These platforms are a rich data source to identify malice, detect spam, and social bots. In IoT, smartphones, laptops, and computers which are portable are used to share data in different platforms which can be used by forensics for investigation on cybercrime [14].

Another approach used by digital forensics is machine learning. Here artificial intelligence that mimic human behavior is used to make work easier. The systems can learn from experience rather than being programmed. Continuous system learning makes it easier to make decisions based on data. Machine learning in forensics is used to identify specific information and obtain knowledge from logic [10] [15]. New information cannot alter existing knowledge obtained. In machine learning algorithms, supervised and unsupervised learning are commonly used. Supervised learning is very easy to understand and implement since data type in labels allows algorithms to predict labels and give feedback if it gives the right answer [10]. Unsupervised learning data is not well structured, has no label, and the system does not know where to go. There is also reinforcement learning which is different from supervised and unsupervised learning in that it learns from mistakes. In this, algorithms provided associate bad behavior to a negative signal and good behavior to a positive signal hence can be supported to prefer good behavior.

Machine learning in forensics operates a huge amount of data to identify criminal actions using artificial intelligence. Algorithms are used to analyze data and know when there is a risk. It enables investigations in huge scattered data set on websites, cloud computing, social networks, and wired networks. Forensics can identify malicious activities from such data, for instance, burglary, intrusion, and money laundering as well as predicting criminal activities from server analysis, wireless devices, and links.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 653-657 www.ijaem.net ISSN: 2395-5252

For SCADA system attack, behavior analysis is used to analyze, identify, and predict anomalies. In cyber-attacks that are highly specialized, the CUmulative SUM (CUSUM) algorithm is used [8] [15] [16].
The CUSUM Equation

$S0 = 0, Sn+1 = \max(0, Sn + xn - wn)$

Sn is the cumulative value sample, n, xn is the value monitored in sample n, wn is the average of monitored value, x is the scan cycle execution detector. This algorithm has been used with great success to detect anomalies in case of cyberattacks.

III. RESULT ANALYSIS

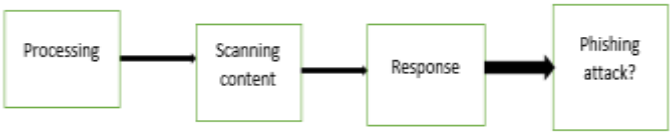
Table 1

Cyberattack and Forensic to Counter

Cyber-attack	Forensics to counter
Phishing attack	The new technique known as PHONEY can be used by forensics to detect and analyze this attack. A web browser extension is used to detect malice or codes misleading URLs. McRae and Vaughn can also be used to detect phishing sites. Intelligence web application firewall (IWAF) ML is also used to detect a phishing attack. URL with electrons (UE) is used to investigate algorithm correlation with different URLs on the internet. The sequence model can differentiate URLs and spam mail.
Ransomware attack	Monitoring tools to detect intrusion early, use of traffic filters. Also, machine and deep learning technology can be used. There is also a hybrid detection model that uses classical and variation auto-encoding that shows activities more precisely.
Protocol attack	For jamming DoS attack detection, jammed area mapping (JAM), model, and cross-layer security check is used. For SCADA attack system detection and prevention are used. Also, the wireless sensor network (WSN) can be checked, message authentication as well as the data encryption algorithms and access protection.
System attack	The SCADA system attack is controlled by using Fieldbus that distributes real-time data control. EtherNet/IP protocol, IO devices settings, and messages not following a specific design control are used to make it hard for the attacker to get details of the system or device. CUSUM algorithm is also used.
Supply chain	ML, AI, and real-time intelligence are used to predict this cyber-attack.

Figure 4

Phishing Phoney



International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 653-657 www.ijaem.net ISSN: 2395-5252

IV CONCLUSION

Cyber intrusions project critical sectors to vulnerability. Criminals use illicit access from organizations that have poor cyber security. Digital forensics has presented a whole new dimension of dealing with cyber-criminal and providing cybersecurity by identifying, detecting, preventing, and recovering sensitive data. Cybersecurity as shown above is dependent on several environmental factors and can be problematic. Complex patterns, systems, and processes that are likely to evolve can cause vulnerability of the system or network. Standardized systems are maintained depending on the age of the system, and complexity. Cybersecurity and forensics take place in three dimensions as shown in the block diagram. First, the cyber threat is identified, then categorized or specified depending on the environment or area of vulnerability depending on the organization. Then finally the forensic approach to detect and prevent cyberattacks or retrieve lost data as shown in the block diagram fig. 2, fig. 3, and fig. 4

REFERENCES

[1] Okereafor, K., & Adelaiye, O. (2020). Randomized cyber attack simulation model: A cybersecurity mitigation proposal for post COVID-19 digital era. International Journal of Recent Engineering Research and Development (IJRERD), 5(07), 61-72.

[2] Montasari, R., & Hill, R. (2019, January). Next-generation digital forensics: Challenges and future paradigms. In 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3) (pp. 205-212). IEEE.

[3] Mathews, J. A., George, G. P., & Dhanalakshmi, M. P. (2020). Analysis of Virtual Machine in Digital Forensics.

[4] Bodeau, D. J., McCollum, C. D., & Fox, D. B. (2018). Cyber threat modeling: Survey, assessment, and representative framework. MITRE CORP MCLEAN VA MCLEAN..

[5] Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations. arXiv preprint arXiv:2103.17028..

[6] https://www.hstoday.us/featured/cyberattacks-on-critical-infrastructure-as-the-new-wmd/

[7] https://www.infosecurity-magazine.com/opinions/cyber-war-critical-infrastructure/

[8] Tsiknas, K., Taketzis, D., Demertzis, K., & Skianis, C. (2021). Cyber threats to industrial IoT: a survey on attacks and countermeasures. IoT, 2(1), 163-188..

[9] Okereafor, K., & Djehaiche, R. (2020). A Review of Application Challenges of Digital Forensics. International Journal of Simulation Systems Science and Technology, 21(2), 35-1..

[10] Iqbal, S., & Alharbi, S. A. (2020). Advancing automation in digital forensic investigations using machine learning forensics. Digital Forensic Science, 3..

[11] Alghamdi, M. I. (2021). Digital Forensics in Cyber Security—Recent Trends, Threats, and Opportunities. In Cybersecurity Threats with New Perspectives. IntechOpen. [10] S. R. Jordan, S. L. Fenn and B. B. Shannon, "Transparency as Threat at the Intersection of Artificial Intelligence and Cyberbiosecurity," IEEE Computer Society, Washington, D.C., 2020, doi: 10.1109/MC.2020.2995578.

[12] Pandi, G. S., Shah, S., & Wandra, K. H. (2020). Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation. Procedia Computer Science, 167, 163-173.

[13] 13. Sapienza, A., Ernala, S. K., Bessi, A., Lerman, K., & Ferrara, E. (2018, April). Discover: Mining online chatter for emerging cyber threats. In Companion Proceedings of the The Web Conference 2018 (pp. 983-990).

[14] Zhang, Y., He, D., & Choo, K. K. R. (2018). BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT. Wireless. Communications and Mobile Computing, 2018

[15] Nguyen, T., Wang, S., Alhazmi, M., Nazemi, M., Estebsari, A., & Dehghanian, P. (2020). Electric power grid resilience to cyber adversaries: State of the art. IEEE Access, 8, 87592-87608..

[16] Venkataramanan, V., Srivastava, A. K., Hahn, A., & Zonouz, S. (2019). Measuring and enhancing microgrid resiliency against cyber threats. IEEE transactions on industry applications, 55(6), 6303-6312.