Applying the Kill Chain and Diamond Models to Microsoft Advanced Threat Analytics

Levent Ertaul, Mina Mousa
California State University East Bay, Hayward, CA, USA
levent.ertaul@csueastbay.edu , mina.mousa@horizon.csueastbay.edu

***Abstract* - Rapidly evolving cyber attacks and inadequate traditional methods of intrusion detection have increased the need for sophisticated threat detection methods. A new generation of intrusion detection methods, including the Kill Chain and Diamond models, have been introduced to detect Advanced Persistent Threats (APT). These models divide the intrusion process into phases and study the connections between the victim, adversary, infrastructure, and capabilities to provide a greater understanding of the nature of the intrusions. Microsoft has introduced Microsoft Advanced Threat Analytics (MS ATA) as a solution for intrusion detection. In this paper, it is observed how MS ATA detects intrusions using the phases outlined by the Kill Chain and Diamond models. It is shown that MS ATA can successfully detect intrusions in both early and late phases of the Kill Chain model.**

Keywords -- Intrusion detection, Microsoft Advanced Threat Analytics, MS ATA, Kill Chain, Diamond model

I. INTRODUCTION

Cyber attacks have existed since the development of the Internet. These attacks have evolved significantly in recent years and ranged from viruses and worms to malware and botnets. During recent years, a new generation of intrusions, the Advanced Persistent Threats (APT) have emerged [1]. Although traditional defenses may be able to keep known intrusions from accessing the network, they are not sufficient against APTs. Therefore, it is essential to develop intrusion detection methods that can continually monitor networks and security controls for their effectiveness [2]. Intrusion detection models such as Anomaly-based [3] and Signature-based [4] have been used with limited success; this is because the adversary learns the actions and signatures that trigger these models and avoids them. The Kill Chain and Diamond models have shown greater effectiveness in detecting intrusions. The Kill Chain model was developed by Lockheed Martin [5]. Three individuals, Sergio C, Andrew P, and Christopher B, built the Diamond model [6]. Both models are widely used, and many organizations have leveraged them as methods for intrusion detection. These two models answer questions about the underlying process of intrusions. Both models are intelligence-driven, and they reveal not only the nature of the intrusion, but also the motive behind it [7].

This paper seeks to demonstrate a connection between the processes used by Microsoft Advanced Threat Analytics (MS ATA) to detect intrusions and the processes used by the Kill Chain and Diamond models. According to Microsoft, MS ATA is a solution that helps protect an organization from multiple types of advanced targeted intrusions and insider threats. MS ATA captures network traffic of multiple protocols to identify intrusions by using MS ATA central and gateway engines [8].

This paper is divided into six sections. Section II will introduce the Kill Chain model and analyze its seven phases of intrusion detection. Section III will describe the Diamond model and discuss its four core features and its meta-features. Section IV describes MS ATA and how it is implemented in a network in order to capture the network's traffic and analyze users' behavior. Section V examines relevant features of MS ATA for intrusion detection in the reconnaissance, command and control phases. The phases are also discussed using the Kill Chain and Diamond models. To conclude, the findings are summarized, and a plan for further research is introduced.

II. KILL CHAIN MODEL OVERVIEW

The Kill Chain model is an intelligence-driven intrusion detection method that has seven phases. These phases enhance the visibility of an intrusion and help security teams understand an adversary's tactics, techniques, and procedures [9]. The phases form an integrated end-to-end process that is described as a chain; breaking any step will interrupt the entire chain. This is shown in Figure 1, where an adversary goes through a series of phases to accomplish his/her goals. A typical APT goes through seven phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives.

Figure 1: Phases of the Kill Chain model .

The phases of intrusion that are presented in Figure 1, are exemplified in Tables 1 and 2, where an adversary sends phishing e-mails to an organization with a malware attachment. Reconnaissance occurs through a phishing e-mail. Then, weaponization and delivery happen through an e-mail attachment delivered to the victim's machine. Afterward, exploitation and installation of the malware take place in the victim's machine. Lastly in the C2 and action phases the adversary is able to take control and act on their objectives [10].

Table 1: Example of intrusion phases.

Phase	Action
Reconnaissance	Phishing e-mail
Weaponization	Attachment
Delivery	Malware
Exploitation	Execute
Installation	Install
C2	Control
Actions on Objectives	Carry out goals

Table 2: Example of intrusion timeline

Phase	Jan.	Feb.	Mar.	Apr.
Reconnaissance	Phishing e-mail			
Weaponization		Attachment		
Delivery		E-mail with malware		
Exploitation			Execute	
Installation			Install	
C2				Control
Actions on Objectives				Carry out goals

Detection of the intrusion could occur during any phase of the intrusion process shown in Tables 1 and 2. Figure 2 shows an early detection, during the delivery phase. Figure 3 shows an example of detection in a later phase, C2.

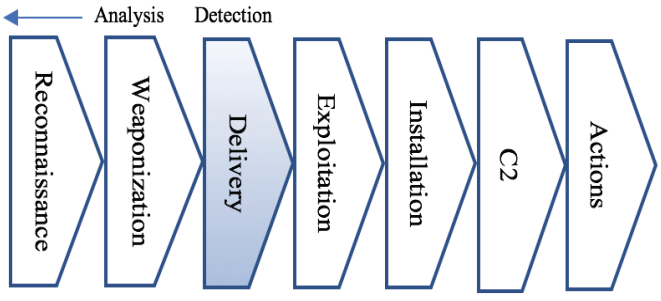

Figure 2: Early detection phases of the Kill Chain model

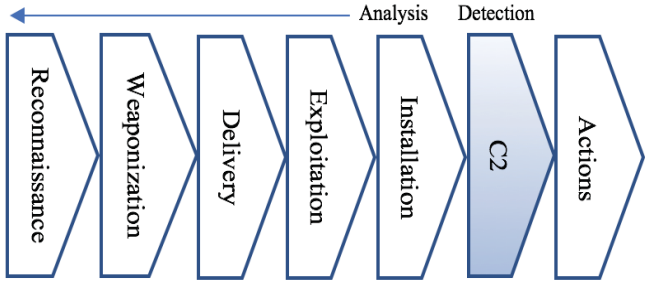

Figure 3: Late detection phases of the Kill Chain model.

The Kill Chain Model is unique in that it combines intelligence from different phases to identify the nature and degree of the intrusion [11].

III. DIAMOND MODEL OVERVIEW

The Diamond model is typically used in conjunction with the Kill Chain model. The Diamond model, in its simplest form, is shown in Figure 4. This model shows an adversary that is deploying a capability over an infrastructure against a victim. These processes are called events [12].

Security analysts use the Diamond model's vertices to discover and detect events. These vertices are connected by edges which illustrate the natural relationships between the features. By pivoting within vertices and across edges, analysts reveal more information about an adversary or the adversary's operations, and can discover new infrastructure, capabilities, and victims. The meta-features shown in Figure 4 are used to capture critical knowledge, when possible, about times of intrusion (both beginning and end), phase, result, direction, methodology, and resources [13].

An event is just one step in a chain that the adversary or adversaries must follow to reach their goals. Thus, events are phase-oriented and connected into activity threads by the adversary-victim relationship. This process symbolizes the course of an adversary's operation. Both events and activity threads are essential elements to provide a complete understanding of malicious activity [14].

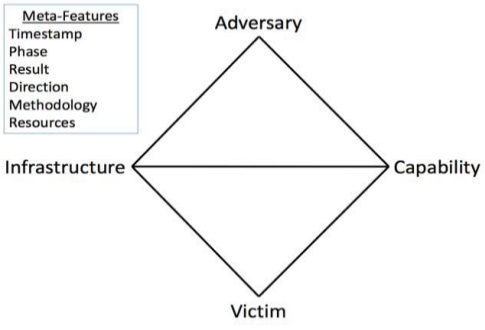

Figure 4: Core and meta features of the Diamond model

A Diamond event describes a discrete, timed activity limited to a specific phase in which an adversary demands external resources and utilizes a capability and methodology over an infrastructure against a victim. Notably, not all features have to be known to establish a Diamond event. Generally, the majority of features are assumed to be unknown and revealed only after the initial discovery.

In a Diamond event, the adversary is the actor or organization using capability against the victim in order to reach their desired goal. In most events, information about the adversary is unknown at the time of discovery. The capability feature explains the tools and techniques used by the adversary in the event. The infrastructure feature explains the logical and physical communication system utilized by the adversary to transport a capability and maintain control of capabilities such as C2. Infrastructure could, for instance, include e-mail addresses, domain names, voicemails, etc. The victim is always the target of the adversary. A victim could be people, organizations, e-mail addresses, domain names, IP addresses, etc. It is recommended to differentiate between the victim's persona and their assets because they fulfill different analytical purposes. For instance, the victim's persona is beneficial in non-technical analyses including socio-political implications; the victim's assets are related to technical aspects such as software vulnerabilities [15] [16] [17].

These four core features (adversary, capability, victim, infrastructure) are connected through a process called analytic pivoting. Analytic pivoting is one of the most powerful aspects of the Diamond model. It helps security teams understand the relationship between core features, which reveals new information about malicious activities [18].

Figure 5 illustrates analytic pivoting as a five-step process. In step 1, the victim discovers malware. In step 2, this malware contains C2 domain. In step 3, the C2 domain resolves to a C2 IP address. In step 4, the firewall logs reveal information about additional victims contacting the C2 IP address. Finally, in step 5, the IP address ownership details reveal information about the adversary or adversaries [19].

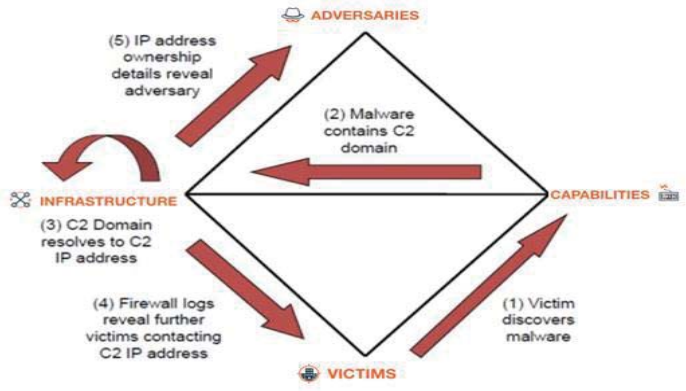

Figure 5: Analytic pivoting using the Diamond model.

The Diamond and Kill Chain models are extremely complementary. The Diamond model helps security teams develop an understanding of how to assemble the necessary information in order to apply the Kill Chain model, while Kill Chain analysis helps security teams understand the phases of the intrusion [20].

Once the security team builds an activity thread based on diamond events, they can identify each event using the Kill Chain model. These activity threads can also help in determining actions needed to remediate an intrusion. Therefore, these threads of activity in the Diamond model allow actions to be planned to protect multiple victims from the activity of an adversary. In the next section Microsoft Advanced Threat Analytics is discussed.

IV. MICROSOFT ADVANCED THREAT ANALYTICS (MS ATA)

MS ATA is an intrusion analytics solution that detects threats and intrusions. By applying the Diamond and Kill Chain models to MS ATA, security teams may develop a deeper understanding regarding the nature of the intrusion. As shown in Figure 6, MS ATA can be placed on the network and receive a mirrored copy of the traffic that is fed to the domain controller (DC). MS ATA has two main components: the ATA Center and the ATA Gateway.

The strength of MS ATA is that it builds a profile for each user. It learns user behavior, helping it detect abnormal activity [21]. Additionally, MS ATA can provide continuous monitoring through advanced algorithms and behavioral analysis. It learns new behaviors from connected users, devices, and available resources [22]. Furthermore, it provides a timeline of events, helping the security team to set priorities. Using the timeline, the security team can see exactly how the attack happened [23]. This increases the productivity of the security team by emphasizing the next steps to be taken [24].

When adversaries start collecting information on the infrastructure the victim is using, MS ATA determines what types of assets the adversary has compromised [25]. It also tracks the adversary's movement during an attack inside the network. Moreover, when the attacker gains information to carry out the attack using different endpoints, credentials, and techniques, MS ATA learns about domain persistence. These attacks include, but are not limited to, Golden Ticket, Pass-the-Ticket, Pass-the-Hash, Reconnaissance, Forged PAC (MS14-068), Brute Force Malicious, Replications, and Remote Execution [26].

As explained in Figure 6, ATA consists of the ATA Center that receives data from any deployed ATA Gateways and/or deployed ATA Lightweight Gateways. The ATA Gateway is installed on a dedicated server that monitors the

traffic from the domain controllers using either port mirroring or Network Terminal Access Point (TAP) [27].

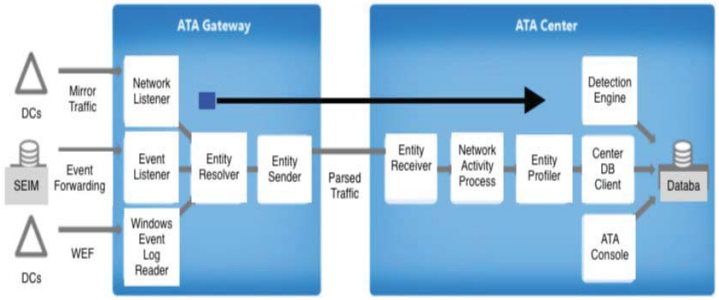

Figure 6: Components of MS ATA

V. EXPERIMENTS USING MS ATA

MS ATA was used in our experiments in both a real and virtual environment. In both environments, a Windows Server 2016 virtual machine was created and ATA Center was installed. Then, ATA Gateway was installed in order to receive mirrored traffic from the gateway.

As shown in Figure 7, ATA Center was installed in the network, where it monitored the domain controllers DC1, DC2, DC3, and DC4. Two ATA Lightweight Gateways were installed on DC1 and DC2 to capture the traffic going through them. ATA Gateway was installed on the gateway of an organization and monitored the network traffic [28].

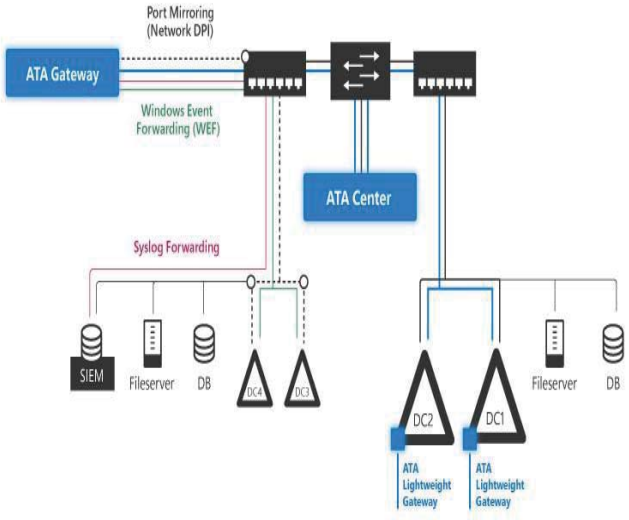

Figure 7: Structure of MS ATA

Three experiments were created to test MS ATA. The first two experiments consisted of intrusions in early phases, such as the reconnaissance phase. The third experiment was created to be an example of an intrusion in the later phases, such as the C2 phase. In the initial two experiments, the ***"Nslookup.exe"*** tool was used first [29]. This tool has a variety of features that can collect information concerning DNS servers, mail servers, subdomains, etc. Then, the ***"NetSess.exe"*** tool [30] was applied, which has the capability to enumerate Server Main Block (SMB) sessions [33]. In the third experiment, the ***"psexec.exe"*** [31] tool was used to execute a program or command on a machine remotely.

The first experiment was conducted to simulate a situation where an adversary logged into a computer on the network, opened a Command Prompt (CMD) [32], and ran ***"nslookup.exe."*** From the CMD window, the adversary ran the LS command to list the DNS zones. As a result, MS ATA initiated a flag, providing intrusion details including who, what, where, when, and how. As shown in Figure 8, MS ATA detected a reconnaissance intrusion.

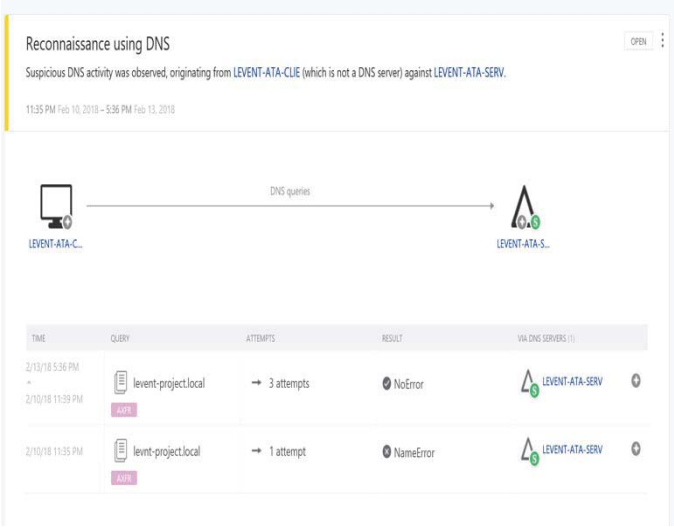

Figure 8: Example of DNS reconnaissance

In the second experiment an SMB Session Enumeration against the Domain Controller (DC) was performed. This type of intrusion is difficult to detect through firewalls because the SMB protocol is widely used. For instance, Windows machines use SMB protocol to communicate with each other and handle resources, including file sharing and printing over the network [34]. In addition, SMB protocol facilitates access to remote Windows services.

The SMB protocol was a target for devastating malware because it is a widely used protocol [35]. This included WannaCry [36], which took advantage of the SMB vulnerability "EternalBlue" [37] to compromise Windows machines. To understand the reaction of MS ATA to SMB intrusions, the ***"NetSess.exe"*** tool was used for SMB Session Enumeration against the DC [38]. Figure 9 shows the results-

- MS ATA generated an alert, giving intrusion details including who, what, where, and when.

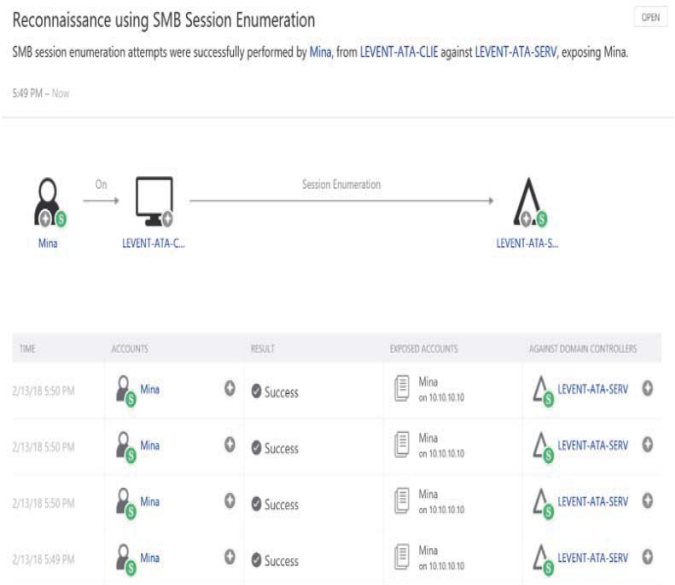

Figure 9: Example of an SMB intrusion

The output from MS ATA in experiments one and two, Figures 8 and 9, shows that an adversary is collecting data about the DNS information and using SMB Sessions Enumeration. The Kill Chain phases can be applied using these results to show that the intrusion is in its reconnaissance phase, as shown in Figure 10.

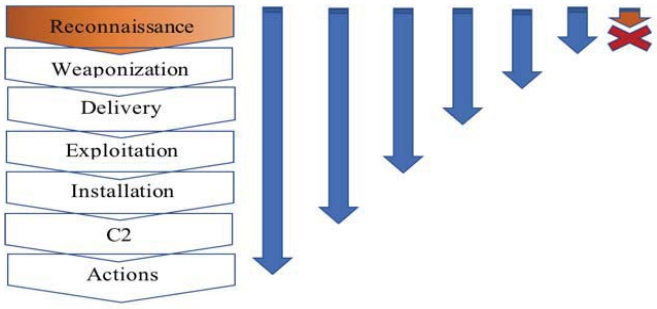

Figure 10: An intrusion in the reconnaissance phase in the Kill Chain model.

Figure 11 illustrates the intrusions in experiments one and two using the Diamond model. In this Figure, the victim's network is scanned by an adversary that has the capability of using the ***"Nslookup.exe"*** and ***"NetSess.exe"*** tools to collect information concerning shared network resources. Using the outputs of MS ATA to connect the main core features of the Diamond model reveals the nature of the intrusion and its capability. MS ATA reveals the IP address used in the intrusion, thus helping to identify the adversary behind it.

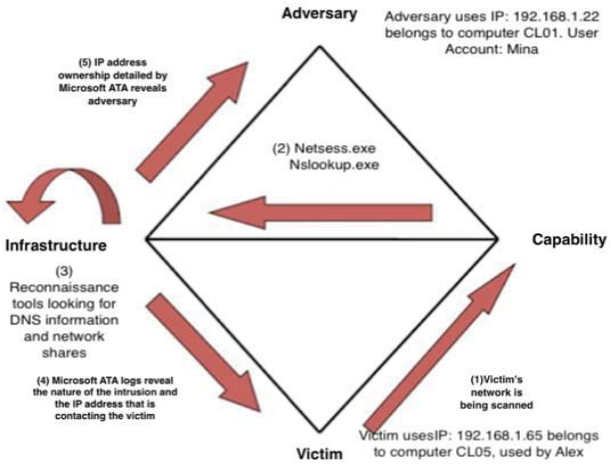

Figure 11: The Diamond model applied to DNS and SMB Reconnaissance Intrusion

In the third experiment, an attempt was made to execute a command on a victim's machine remotely. For this type of intrusion, the ***"psexec.exe"*** tool was used to execute the command, and it attempted to create a new user account. Figure 12 shows the response of MS ATA: "Remote execution attempt detected."

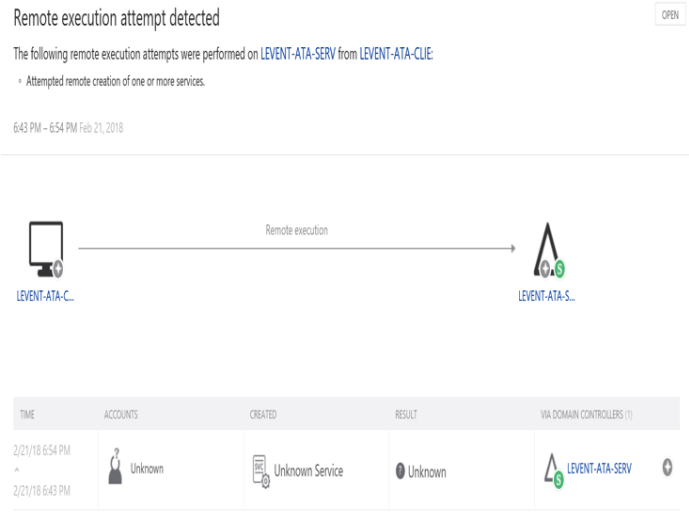

Figure 12: Example of remote execution attempt

The extracted information from the third experiment, Figure 12, can provide security teams with much of the needed information to apply the Kill Chain and Diamond models. This will enable them to gain a deeper understanding about the phase and nature of the intrusion. Figure 13 describes this intrusion using the Kill Chain model. Here, the adversary was able to successfully reach the C2 Phase to install the ***"psexec.exe"*** tool on the victim's machine, and then use the tool to execute commands on another machine in the network.

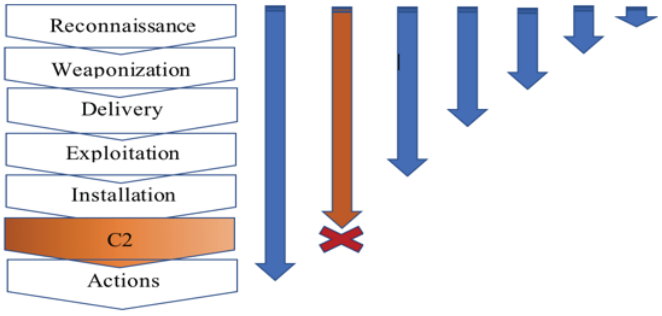

Figure 13: An intrusion in the C2 Phase of the Kill Chain model

In Figure 14, the Diamond model shows that in experiment three, the victim's computer is being controlled by an adversary in order to remotely execute a command or a file on other machines in the network. Here, MS ATA detects the attempted remote execution and reveals the details concerning the intrusion. Details about the IP address help identify the adversary or adversaries. Furthermore, the Diamond model shows the connections between the adversary and victim, and the infrastructure used by the adversary, along with the capability used during the intrusion. This shows that MS ATA provides much of the information that is needed to apply the Diamond model.

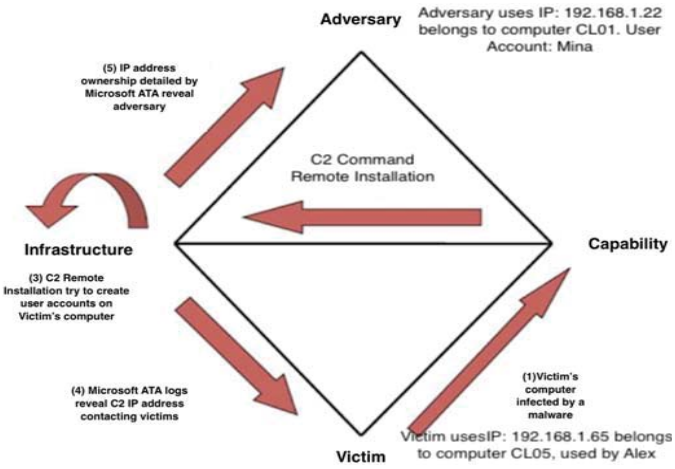

Figure 14: The Diamond model applied to the C2 intrusion

In reality, an organization cannot prevent every attack. It becomes more difficult when the adversary has access to a variety of tools and the organizational infrastructure to carry out the attack. For this reason, quick intrusion detection can prevent both internal and external adversaries from achieving their goals. Using MS ATA in conjunction with the Kill Chain and Diamond models gives security analysts the advantage of looking at the big picture and understanding the full process. For instance, in the three experiments we performed, DNS, SMB, and Remote Execution intrusions may seem normal for security analysts. However, by applying the Kill Chain and Diamond models we received a deeper understanding of the phases and nature of the attacks. As shown in Figure 15, the information that was provided by MS ATA made it easier to get the needed information from one place instead of collecting it from multiple recourses. Therefore, detection and response should be faster and more efficient.

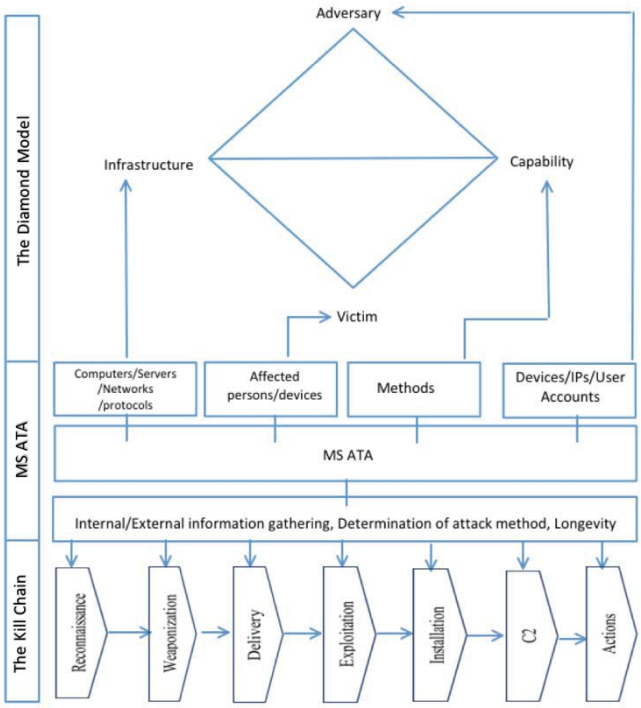

Figure 15: Integrating MS ATA to The Diamond and Kill Chain models

VI. CONCLUSION

When using intrusion detection models, security teams seek to use models that incorporate intelligence in the detection process. The Kill Chain and Diamond models help analysts understand the underlying nature of an intrusion and classify it into phases. Additionally, tools and solutions, like MS ATA, can assist them to utilize these models effectively.

In this study, it was shown that MS ATA was successful in detecting intrusions in their early phases, such as reconnaissance, through collecting DNS information and SMB Session Enumeration, and in late phases, such as the C2 phase, through remote execution. It was shown that MS ATA presented its results in ways that can help security teams effectively apply the Kill Chain and Diamond models. Using MS ATA in conjunction with the Kill Chain and Diamond models will help security teams better understand the complexity of an intrusion, its phase, and the relationships between the adversary, victim, capability, and infrastructure. Given the effectiveness of using MS ATA and applying Kill Chain and Diamond models to it, future research will include comprehensive analysis of new releases of MS ATA.

VII. REFERENCES

[1] Haq, Thoufique, Jinjian Zhai, and Vinay K. Pidathala. "Advanced persistent threat (APT) detection center." U.S. Patent No. 9,628,507. 18 Apr. 2017.

[2] Ussath, Martin, et al. "Advanced persistent threats: Behind the scenes." Information Science and Systems (CISS), 2016 Annual Conference on. IEEE, 2016.

[3] Garcia-Teodoro, Pedro, et al. "Anomaly-based network intrusion detection: Techniques, systems and challenges." computers & security 28.1-2 (2009): 18-28.

[4] Beigh, Bilal Maqbool. "One-stop: A novel hybrid model for intrusion detection system." Computing for Sustainable Global Development (INDIACom), 2014 International Conference on. IEEE, 2014.

[5] Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research1.1 (2011): 80.

[6] Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz. The diamond model of intrusion analysis. Center for Cyber Intelligence Analysis and Threat Research Hanover MD, 2013.

[7] Rid, Thomas, and Ben Buchanan. "Attributing cyber attacks." Journal of Strategic Studies 38.1-2 (2015): 4-37.

[8] Saldana."Advanced Threat Analytics Documentation." docs.microsoft.com/en-us/advanced-threat-analytics/.

[9] Title. (Cyber Kill Chain). Retrieved February 28, 2018, from https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

[10] "Newsletters."EventTracker,www.eventtracker.com/newsletters/siemphonic-cyber-kill-chain/

[11] David Sweigert, Defensive cyber security expert Follow. "Understanding Cyber Kill Chain and OODA loop." LinkedIn, 11 Jan. 2017, www.slideshare.net/dgsweigert/under-cyber-kill-chain-and-ooda-loop.

[12] Faulkner, Sophia A. Looking to Deception Technology to Combat Advanced Persistent Threats. Dis Utica College, 2017.

[13] Cunningham, Dr. Chase. "Evolution of the online battlefield."

[14] "Building Threat Hunting Strategies with the Diamond Model." Active Response, 13 Oct. 2016, www.activeresponse.org/building-threat-hunting-strategy-with-the-diamond-model/.

[15] "Journal of Computer Science IJCSIS Vol.10 No. 9 September 2012.www.scribd.com/document/109920301/Journal-of-Computer-Science-IJCSIS-Vol-10-No-9-September-2012.

[16] Rittenberg, Josh . "The Rise of Threat Hunting in Preventing Cyber Attacks." Breach , 14 Mar. 2017, breachmemo.com/the-rise-of-threat-hunting-in-preventing-cyber-attacks/.

[17] Stech, Frank J., Kristin E. Heckman, and Blake E. Strom. "Integrating cyber-D&D into adversary modeling for active cyber defense." Cyber Deception. Springer, Cham, 2016. 1-22.

[18] Spring, J. M. (2014). Toward realistic modeling criteria of games in internet security. Journal of Cyber Security & Information Systems, 2(2), 2-11.

[19] Kotheimer, John, and Kyle OMeara. Using Honeynets and the Diamond Model for ICS Threat Analysis. No. CMU/SEI-2016-TR-006. Carnegie-mellon university of Pittsburgh,USA, 2016.

[20] Posts about diamond model on Count Upon Security. (Diamond Model). Retrieved January 28, 2018, from https://countuponsecurity.com/tag/diamond-model/

[21] Security, S. M. (MS ATA.). Microsoft Advanced Threat Analytics (ATA) Overview. Retrieved January 15, 2018, from https://adsecurity.org/?p=1583

[22] Beaver, Kevin . "Advanced Threat Analytics uses self-Learning algorithms to compare normal user behavior to what is currently happening in an Exchange environment." Tech Target, 1 Feb. 2018, searchexchange.techtarget.com/tip/How-Microsoft-Advanced-Threat-Analytics-helps-secure-Exchange.

[23] Joos, Thomas "Security analysis with Microsoft Advanced Threat Analytics Under the Radar" http://www.admin-magazine.com/Archive/2016/32/Security-analysis-with-Microsoft-Advanced-Threat-Analytics

[24] Security, S. M. Microsoft Advanced Threat Analytics (ATA) Overview. Retrieved February 11, 2018, from https://www.linkedin.com/pulse/benefits-using-microsoft-advanced-threat-analytics-neil-coughlan/

[25] Beaver, Kevin . "How Microsoft Advanced Threat Analytics helps secure Exchange." Tech Target. Principle Logic, LLC, Web. 1 Feb. 2018.

[26] Smith, Russell . "What is Microsoft Advanced Threat Analytics (ATA)?"| Microsoft Docs, docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata.

[27] "Connecting Microsoft Advanced Threat Analytics to Azure Security Center." Microsoft Azure. Microsoft, 5 Jan. 2018. Web. 14 Mar. 2018.

[28] "What Is Microsoft Advanced Threat Analytics?" Petri, 2 Feb. 2017, www.petri.com/microsoft-advanced-threat-analytics.

[29] "Nslookup.exe." Nslookup.exe Windows process - What is it?, www.file.net/process/nslookup.exe.html.

[30] NetSess, www.joeware.net/freetools/tools/netsess/index.htm.

[31] Sanders, Chris. "PsExec and the Nasty Things It Can Do." TechGenix, TechGenix, 9 Sept. 2017, techgenix.com/psexec-nasty-things-it-can-do/.

[32] Fisher, Tim. "What Is the Command Prompt in Windows, and How Do I Open It?" Lifewire, www.lifewire.com/command-prompt-2625840

[33] "SMB." SMB (Server Message Block) Definition, techterms.com/definition/smb.

[34] Sharpe, Richard. "Just what is SMB?." Oct 8 (2002): 9.

[35] Miller, John. "WannaCry Ransomware Campaign: Threat Details and Risk Management « WannaCry Ransomware Campaign: Threat Details and Risk Management." FireEye, www.fireeye.com/blog/products-and-services/2017/05/wannacry-ransomware-campaign.html.

[36] Burgess, Matt. "Everything you need to know about EternalBlue – the NSA exploit linked to Petya." WIRED, WIRED UK, 29 June 2017, www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch.

[37] Islam, A. (2017, May 26). SMB Exploited, WannaCry Use of "EternalBlue". Retrieved February 25, 2018, from https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.htm

[38] "Net Cease - Hardening Net Session Enumeration." TechNet Net Cease - gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dcb5b.