Prediction of Adversary's TTP using Caldera

Diana Arulkumar, Kartheeban.K.

Abstract*: Due to the ubiquity of the internet in all the lines of the disciplines, cyber security becomes essential in day to day life. To make the cyber assets resilient from the challenging attacks like Advanced Persistent Threats (APT), the experts needs a strategic rules and proactive decision-making models The Caldera is a adversarial emulator for both blue and red team to test the APT along with the cyber kill chain(CKC).The resilience could be achieved when the blue team and red team work together in analyzing the cyber threats based on the probabilistic of creating adversarial profile with different characteristic helps in finding the priority of the assets of the organization from the point of an adversary in launching the cyber -attack.

Keywords— Adversarial emulator, Advanced Persistent Threats (APT), cyber kill chain(CKC) ,caledra, cyber-attack..

I. INTRODUCTION

Due to the development of Industrial 4.0 technologies like IoT, smart devices, smart environment, cloud, fog, edge storages, etc., need to protect the multifarious components of the applications, the cyber security is essential in cyber-network. [1] Devices connected in the cyber network like PC's, hub, modem, routers, firewall, servers and IDS, data -centers and so on are tend to be vulnerable and highly probable assets to be targeted with the huge range of threats. Even many of the protective shield like antivirus, continuous monitoring fail to protect the legacy systems and unpatched systems. Since the adversarial tries to launch the breaches through the variety of threats for political gain, financial gain and out of the own curiosity. Among the different exploiting techniques of adversarial, the state sponsored sophisticated cyber-attacks is used to damage the assets and exfiltrate the sensitive data for the sake of political and economic gain.

To provide resilient in the cyber network from the threats, risk analysis of the cyber-attacks necessary to be studied with the NIST framework such as i) identify the asset, ii)prioritize the asset , iii)continuously monitor and detect the threats and the vulnerability of the assets , iv)respond to the incident immediately for the consequences v) recover by forensing the adversarial event. [2] One of the examples of critical areas like Industrial control system (ICS) are prone to targeted by adversarial because of operations of legacy systems. The ICS has a greatest challenge in protecting the assets from modern sophisticated attacks.[6]The framework widely used in finding the risk metric is Probability Risk Analysis (PRA) [Jensen 2002],

Risk = threat × vulnerability × consequence (1)

The cyber experts will estimate the probabilities of threat and vulnerability and consequence is calculated by the incurred cost of the threat. [5,7,8] The existing defense used the signature matching in detecting typical APT example threats like Stuxnet, Operaton Aurora, Duqu, Flame, Red October, Miniduke are insufficient in measuring the cyber-attack. As many enterprises put the effort in developing cyber defense mechanism like [2,9] (STRAM) Security, Trust, Resilience, and Agility Metrics security framework is used to estimate the number of compromised nodes in the cyber network.

The cyber threats are assessed with various tools such as Vulnerability Assessment (monthly / quarterly), Penetration testing (1or 2 weeks) and Red Teaming (3 to 4 weeks or more longer). It is observed that among all the assessment tools, red teaming is considered to be more effective to identify the type of vulnerability for the cause of cyber threats and investigate the vulnerabilities with the challenging competence of team players.Thus, the red teaming supports in large range of real-world applications such as self-driving cars, robotics, resource management, education, and so on. To resist the adversarial activities, Adversarial machine learning technique is considered predominantly as important for security life-threatening systems.

The paper is focused on the Advanced Persistent Threat (APT) which targets the assets of corporate /individual/government organization that tend to launch the attacks by the adversarial in phases and remains passive for a longtime. The challenge of the red teaming is to find the undetected and passive APT which compromise the system and controlled using C2 channel commands for (data modification, stealing) data exfiltration. The caldera provides an understanding of the process of APT and enables to create the adversarial profile in launching the attack based on the adversarial knowledge by selecting the characteristics.

The paper structure is as follows. In Section 2 related works of the adversarial emulator tools in each phase of operational process of red and blue team is explained. In section 3, adversarial TTP's along with CKC is described. In Section 4 The operational process is experimented with caldera. In Section 5, results and discuss in is discussed and finally conclusion. in Section 6

II. RELATED WORKS

A. *Adversary emulation tools*

Building a better model for security with the generators act as adversarial (redteam) and defenders act as a security analyst (blue team) using adversarial emulators.[10,11,14] Network resilience test against the advanced persistent threat is proved with the automatic adversary emulator. The Tactis, Techniques and the Procedures followed by the

Revised Manuscript Received on December 16, 2019.

Diana Arulkumar*, Computer science, Karunya Institute of Technology and science, Coimbatore, India. Email: dianacse@karunya.edu

Kartheeban.k, Computer science, Kalasalingam Academy of Research and Education , Srivilliputtur ,India. Email:k.kartheeban@klu.ac.in

adversarial are embedded with the cyber kill chain to focus on the objective of the target network.

1) Redteam:

Annually organized to assess the state-of- security level of the organization. The goal is to achieve the resilience with the feedback of periodic assessment from misuse attacks. fig.1 creates the report of vulnerability and Indicator of compromise.`

- Bloodhound

The Pentesters or the red teamer in the enterprize uses Bloodhound to map the privileges with the attack graph which paths from low privilege to high privilege of the users/computers to access the data assets. It maps between groups, devices, users, sessions and access.

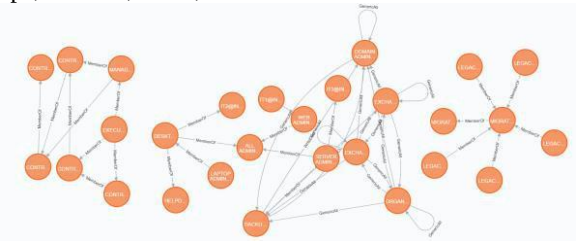

Fig. 1.Blood hound attack graph for privileges[16]

The graph of the Bloodhound is given in fig1 shows the attack graph of Blood Hound Example DB.graphdb and proved very resilient.

- APT Simulator: It can simulate the cyber threat like in a real-time. It is written in windows batch script contains tools and reflect the files as same as compromised.
- Caldera

It is a tool for an adversary emulation of post-compromise. The planning system of caldera respond immediately to the incident with its available solution for the malicious event.

- Empire

A post-exploitation toolkit, in align with the cyber kill chain, the agent has the potential control over compromised machines in executing attacks also includes the privilege escalation and credential theft by overwhelming operation of the Death Star in mapping an attack path to be persistence to till the lateral movement to be the administrator.

2) Blue team:

It deals with the daily incident event as internal security analyst in Fig 2.It creates the static detection and characterize the malicious behavior.

- *DumpsterFire:*Tool is developed in pythonwith menu driven and to run ascross-platform for customization, time delay, disseminated security events. the blue team can be trained with easily develop a custom event by the redteam to distract,trap the incidents and also the operation scalability.
- *flightslim:* Like wireshark ,malicious network traffic can be generated and security analyst analyse controls and visibility of the network. The tool used to simulate DNS tunneling, C2 command for known target, and other suspicious traffic pattern.

Fig. 2.Cyber kill chain of a) Red team and b) Blue team

The Experts team suggest that purple team is the cross of Red and the blue team in each phase mutually can exchange trial and error method in fixing the target priority from the adversarial perspective. Fig 3The purple team by sharing the information between about security system pave a path to be

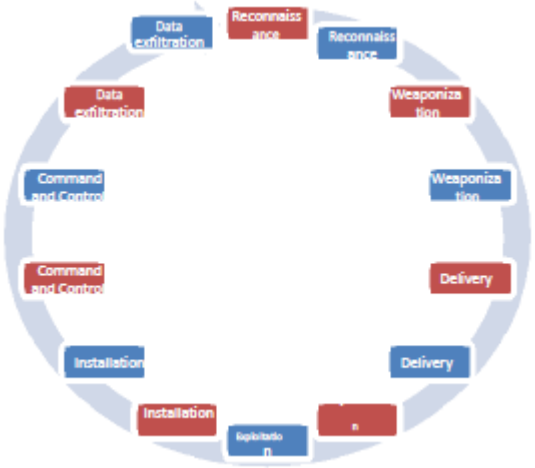

Fig. 3.purple team of APT Life cycle.

Resilient against the adversarial the behavior and APT attack life cycle. The resilience from the APT attack of each phases could be viewed by the security analyst (blue team) through the vulnerability report and Tactics, Tools and Procedure (TTP's) to give a high competent to the adversary in targeting the assets. Therefore, the adversarial emulator helps both the testers in protecting and identifying the assets.

3) Online Forums and CTI reports

In recent days , due to enormous available of accessing resources and evolution of innovating technologies, anyone who are interested in any type of hacking can involve themselves in exploring the TTP's used by the hacker communities can acquire their knowledge through forums, IRC, carding shops etc.,[21].On day today basis, the exploits are increasing and made as commercialization [22]and become lively for hacker community.

[24]Cyber-attacks affect the global economy of many billion dollar in preventing from [18] execution of malicious tools like trojans, zeus, ransomware and keyloggers, SQL injections, and DDoS from United States, Russia, and China. To prevent the cyber-attacks the vendors like FireEye, Cyveillance, Symantec, McAfee, Trend Micro, Sophos, and Kaspersky involved in the generation of Cyber Threat Intelligence (CTI) reports. The CTI reports contain information about network logs, antivirus logs, honeypots, database access events, system login attempts, and intrusion defense system/intrusion protection system (IDS/IPS) events but it will not address the details of the techniques used by the hackers and profile of the threat actors proactively.

The cyber threat Intelligence is used to act proactively toward detecting the zero -day attacks using machine learning techniques against the hackers.

[18]Since in the existing approaches followed by the Academia, research communities and CTI report generation are reactive instead it has to be proactive in composing the information from the forums of online hackers including the tools and adversaries' profile. There are many hacker's forum available online to exchange the knowledge and the content of the tools and the techniques used in the attack patterns(For example, U.S. forums mainly deals with cybercrime and general hacking, Russian forums focus on underground economies and data breaches, Chinese forums share about cyber warfare and virtual goods) .The participants in the forum maximum are unskilled and novices can be develop to skilled high level of profile by accessing through posted link of keywords or phrases which enables the users can access the information and also share hyperlinks, pictures, videos, source code, attachments to disseminate the malicious.

III. ADVERSARIES TOOLS ,TECHNIQUE AND PROCEDURE(TTP'S)

A. *Threat actor*

The case studies are used build the profiles of the APT actors by analyzing their motivations and to group in them category. [12,15]Also, Tactics Technique and Procedure (TTP) is enabled to identify the skill levels, fixing the target as geographic, opportunistic, stealthy behavior. Based on the resources available with attacker attribution and objectives will be affixed. The threat actor matrix will be created and data will be furnished to identify focus of the attacker in launching an effort. The Cost-benefit framework enables to analyses economically to model threat actor by plotting threat actors with feasible targets. The Cost benefit ratio is defines as combination of (M)Expected monetary benefit and (Pb) Expected psychological benefit to the (LBC) Logistical Burden with respect to Skill level,(to architect project and to develop code), Team size (total number of people involved with various skills), Resource cost(required to implement the project) and Time (to schedule various activities in order)

$$\frac{M_b + P_b}{LB_C} \geq 1 \qquad (2)$$

B. *Threat Breaching Techniques*

There are different breaching techniques were employed in network through the various modes such as Hacking(H), Error(E) ,Malware(M), Misuse(Mi), Physical(P), Social(S) to target the data.

TABLE I. BREACHING TECHNIQUES

Breaching techniques	H	E	M	Mi	P	S
Adminware						
Backdoor			✓		✓	
Bribery						✓
Brute force	✓		✓	✓	✓	
Capture app data	✓	✓	✓			✓
Capture stored data	✓					
Data mishandling			✓			
Desktop sharing	✓		✓			
Direct install						
Disabled controls			✓			
DoS	✓		✓			
Download by malware			✓			✓
drive-by						
Email						✓
Email attachment			✓			
Email link				✓		
Email unknown					✓	
Exploit vulnerabilities			✓			
Export data			✓			
Foot printing	✓					
In person		✓				
Knowledge abuse				✓		
LAN access						✓
Loss				✓		
Misconfiguration						✓
Mis delivery				✓		
Partner	✓		✓			
Partner facility			✓			
Password dumper					✓	
Phishing			✓			
Phishing						✓
Phone						✓
Possession abuse				✓		
Pretexting						✓
Privilege abuse			✓			
Personal vehicle			✓			
Physical access			✓			
Public facility						✓
Ram scraper			✓			
Ransomware			✓			
Remote access			✓			
Skimmer					✓	
Spyware/Keylogger				✓		✓
SQLi	✓	✓				✓

Surveillance					✓	✓
Tampering					✓	✓
Theft					✓	✓
Use of backdoor or C2	✓				✓	
Use of stolen credentials	✓			✓		
Victim grounds					✓	
Victim public area					✓	
Victim work area					✓	
Website				✓		
Web application	✓					

Cyber threat intelligence:

[17] CTI has four types, strategical, operational, tactical, technical. Fistly the strategical CTI is information needed by the decision makers for identification and to analyse the risks and its impact. Secondly the operational CTI, the collection of recently identified vulnerabilities and zero-day attacks from the forums of hackers and dark web. thirdly the Tactical

CTI, is used to find the TTP' of Cyber threat actors. The threat actors (TA) who are targeting the resources like network and operating system spends considerable effort in developing the tactics in launch an attack. Since it is difficult for the adversary to develop a new TTP for each time and to launch at the time of attack. So the security analyst (blue team) has to develop the knowledge of the threats and its behaviour associates with the attack patterns are regularly repeated with different combinations. Lastly the Technical CTI, for implementing the types of indicators of compromise (IOC) in various devices such firewall and IDS using the indicators like IP,Hash,C2 channels, artifacts. Among the four CTI the tactical and strategical are essential.

Cyber kill chain (CKC)

The skeleton of an APT was modeled as 'Cyber Kill Chain' coined by Hutchins, Cloppert and Amin of Lockheed Martin3 to realize and examine about an intrusion [5,7] The chain contains phases as

- Reconnaissance - The attacker will gain knowledge of an organization's vulnerability to fix the target through social engineering, spear phishing, Web crawling of Twitter, Facebook, Linked In. Some of the targets are industrial/manufacturing, pharmaceutical, construction, education and IT sectors.
- Weaponization – Using the exploit tool RAT and Trojan (ex: Havex trojan) are packed and it will be sent along with the payload (shellcode, NOP, ROP) to the targeted victim through drive by download, watering hole etc., c)Delivery - Lockheed Martins has identified the most usually following three ways of transporting is sending email, illegitimate websites and infected USB sticks. More popular one among is spear phishing.
- Exploitation – Once the malicious code of attachment file (PE files) in email's payload is executed, the exploit (e.g. CVE-2011-0611 and CVE-2010-2883) will be triggered.
- Installation –Acquiring the access of targeted system by using the stolen credentials helps in mounting Trojans, new back doors and/or for privileges.
- Command & Control (C2) – The installed software now attempts to link to a C2 server; thus, systems will be compromised. Later, targeted system will be started to respond to the commands issued by attackers through the
- network. Since most of the outbound communication, firewall is considered as less reliable and also vulnerable to the attack.
- An action on Objective – The act of negotiating data integrity or availability implies that the adversary was focused for ex-filtrating the data.

TABLE II. COURSE ACTION MATRIX

Phase	DET	DEN	DIS	DEG	DEC	DES
R	Web	Firewall				
W	analytics	ACL				
D	NIDS	NIPS	In-line AV	Queuing		
E	Vigilant user	Proxy filter	DEP			
I	HIDS	Patch	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
A	Audit log			Quality of Service	Honey pot	

Table I portraits the matrix . Detect(DET), Deny(DEN), Disrupt(DIS), Degrade(DEG), Deceive(DEC), Destroy(DES) and Reconnaissance(R), Weaponization(W), Delivery(D), Exploitation(E), Installation(I), Command to control (C2), Actions on Objectives(A) that helps to hardening the system against the traditional security measures also alert the users to behave proactively against the adversaries.

[7] In March 2009 ,the Lockheed Martin Computer Incident Response Team (LM-CIRT) has experimental case study on attempts of three intrusion by an adversary used Tactic: All three intrusions leveraged a common APT tactic: targeted malicious email (TME) delivered to a limited set of individuals, containing a weaponized attachment that installs a backdoor which initiates outbound communications to a C2 server.TTP is about adversaries behavior and attack patterns,which is effective in detecting attack vectors and the cyber threat actors.Many of the adversaries use TTP's in various combination and with the same TTP's with regular practice.

In the table II,[29] Matrix it relates the APT groups and the usage of CKC, in launching the attack. Every APT group focuses on their targets for different purposes through different tactic and techniques which is available for the perpetuality at the instance. From the table, most probably APT groups using the spear phishing for the first step in the launch pad. Based on their knowledge the techniques are employed for various purposes, to target the specific targets.

The targets are not specific, but any organization or software or any process can be controlled using the backdoor activities of the adversaries. The Cyber threat actors are criminals, hacktivist, insider and APT actors. The APT Actors are sophisticated and high profiled attackers act as a group in targeting the assets. The assets are stoned with the adversary's knowledge, skills and resources in implementing the attacks through each phase. As a red team, the members are identified to protect the assets of the organization which could be vulnerable to target by the adversary.

TABLE III. APT AND CKC MATRIX

Phase	APT 16- China	APT 17- China	APT 1 China	APT3 China	APT 30 China	APT28 (Fancy Bear) Russia	APT29 (the Dukes) Russia
Reconnaissance	Spear phishing		Spear-phishing	Spear-phishing	Social engineering	Email credentials spear phishing (outlook web access)	Spear-phishing email with zip file
Weaponization	Malware		Shadyrat trojan	Attachments		Sourface / coreshell (sofacy / Sednit) malware/	Mini duke and Onionduke malware campaigns.
Delivery					Remote payloads in memory	Remote payloads in memory with Firefox bootstrapped	
Exploitation	Cve-2015-2545			Return Oriented programming (rop		Long-term persistence techniques	
Installation			Winhelp files				Cozyduke dropper
C2	Command and control channel	(covers all the phases)hikit generation 2 tool	Barkiofork backdoor,	Pirpi backdoor	Two-stage command and control/ hdoor tool	X-agent (chopsticks)	Cloud storage Services (twitter GitHub, or other storage services) along with malware images
Actions on Objectives	Taiwanese media Organizations	Aurora attacks against Google	Aerospace industry	Internet Explorer Exploits	Backdoors' data Exfiltration of air-gapped networks	Ukrainian application on Android smartphones.	Elections

TABLE IV. TYPES OF INDICATOR

Types of Indicator	Indicators/IOC level	Threat intelligence	Persistence	Efforts of Adversary	Mitigated	Footprints
Hash values (Unique references of sha1, md5.for the sample files)	Computed/ Low	Technical	Short time or immediate	Fuzzy hashes	Intrusion detection and firewall rules	fixed format
Ip addresses	Atomic/ Low	Technical	Short time or immediate	Dynamic IP address	Intrusion detection and firewall rules	fixed format
Domain names (a sub- or sub-sub-domain)	Atomic/ Low	Technical	Short time or immediate	Lax registration standard	Intrusion detection and firewall rules	fixed format
Network artifacts (Uri, c2 channel commands)	Atomic/ Low	Technical	Short time or immediate	Reconfigure and/or recompile tools	Intrusion detection and firewall rules	fixed format
Host artifacts (Registry keys or values known to be created by specific pieces of malware, files or directories)	Atomic / Low	Technical	Short time or immediate	Reconfigure and/or recompile tools	Intrusion detection and firewall rules	fixed format
Tools (Spear phishing, backdoors used to establish C2 or password crackers)	Behavioral/High Attack signatures of threats	Tactical	long-term	research development and training	Investigation process	Change attack patterns
Tactics, Techniques and Procedures (ttps) (From reconnaissance all the way through data exfiltration)	Behavioral Attack signatures of threats/ High	Tactical	long-term	Most time-consuming	Investigation process	Change attack patterns

The pyramid of pain

The Pyramid in fig.4 associates the type of indicators and effort needed to detect the activities of adversarial. From the bottom to top the effort needed to adapt to the environment for the adversarial is increased. The least effort to adapt is significantly more. [13,15] The successful launch of the trivial for file hash and Internet Protocol (IP) address. while it climbs up towards apex the TTPs effort needed to adapt is

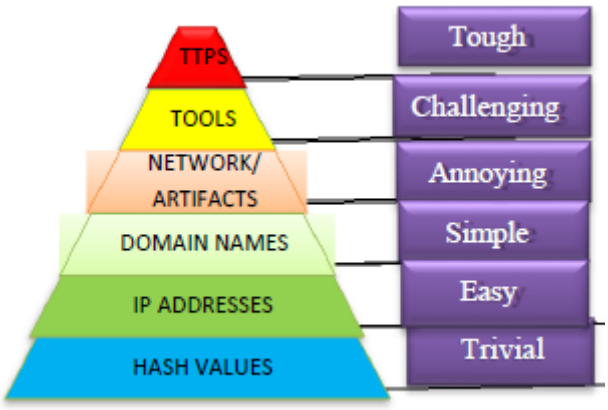

Fig. 4. The Pyramid of Pain

Table III, shows that the Indicator of compromise (IOC) acts as an attack patterns of malware and .[11,15]APT in causing the Incidents of Data breach in cyber network. The pain of adversary to launch a successful target is to make them to work on TTP's to really very much time consuming in every phase of the CKC. [7] Atomic - Atomic indicators can be remain as an intrusion activity and cannot be modular further into small segments. Computed - Computed indicators are extracted from the data involved in intrusion. Behavioral - Behavioral indicators are aggregation of both computed and atomic indicators, analyzed with its quantity and also follows combinatorial logic

IV. ADVERSARY EMULATOR TOOL

CALDERA is developed on MITRE ATT&CK [14] framework as an automated adversary emulation tool, to behave as adversarial to post-compromise in the cyber networks. It can be used by red and blue teams

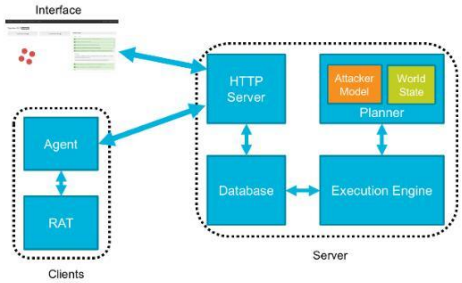

Fig. 5. MITRE caldera the automated cyber adversary emulation system

From Fig 5 Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) framework is created by MITRE.

It has three components Caldera servers, agents and crater. It can be implemented in both the environment of windows and Linux. Adversary emulator operations can be done by creating the network and accessible by all the computers.

TABLE V. TECHNIQUES USED IN CALDERA EMULATOR

Phases of cyber kill chain	Techniques employed
Reconaissance	Social engineering, spear phishing
Persistence	Registry autorun keys, Scheduled Task, Services
Privilege Escalation	Weak service perms, Weak service file perms, Unquoted paths (Path interception)
Defense Evasion, Credential Access	Scripting, Timestamping, Credential Dumping
Lateral Movement	Remote File Copy, Windows, Admin shares, Pass the Hash, PS Exec
Discovery	Remote System Discovery, Local Network config, Registry, Account, System information, Processes/services, System Owner, Permission Group, Files
Execution	PowerShell, Scheduled Task, WMI, SC (service controller
Exfiltration	HTTP/s, Lateral movement

he server can be installed using the docker and the agents may windows OS of version above 8. crater will be a Administrator. The planner creates a various possible with techniques and tactics for each CKC to execute the operation in each phase which is listed in tableIV ATT&CK matrix

APT attack in the network

After login to the caldera server, calendar automates APT in the synthetic and real time environment from the debug menu, connected agents are listed and select a agent to the remote host. To visualize the network, name the network and define the number of hosts. From the threat menu, name the threat and select the features of the threat for the operation and thus the adversarial profile is created. the operation is defined payload with explorer.exe.

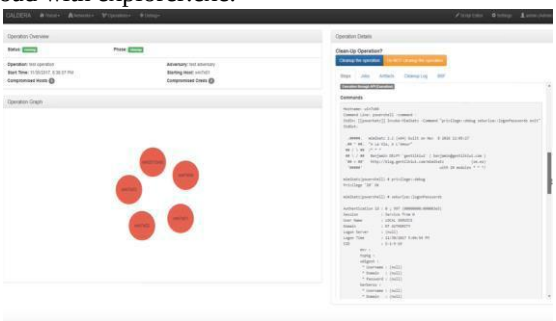

Fig. 6. Mimi Katz is used to dump the credentials of the host in the network

Eventually the system is compromised and enumerating the information of the other host in the network and thus

Adversary control the network. After cleaning the operation, click the artifacts, the operational details of files and processes are listed. Based on the threat technique, the adversarial profile configures the behavior and determine technique in the attack matrix. Fig 6 From the threat tab, click the view details, how attacks map logically relates one another.Attack is a knowledge based of adversarial behaviour, the boxes in green specifies that different techniques used for that phase attack in the ATT&CK Matrix coverage. The matrix has the phases listed in the table V with its different techniques used by the adversarial knowledge.

V. RESULTS AND DISCUSSION

The caldera is used for generating the adversary profile in order to analyse the types of attack techniques used by the adversaries. Based on the names of the threat and select the features of the threat for the operation and thus the adversarial profile is created. Caldera generates the plan based on the MITRE's Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) and a pre-configured adversary model. Caldera's feature which dynamically varies its behavior to represent human adversaries to perform an operation over a system. As an open source tools, it also groups as penetration testing or security auditing tools.

The action plan for creating the adversary profile are determined in [29] customizable Markov decision processes (MDPs) heuristic to calculate the score.

TABLE VI. ACTION PLAN FOR ADVERSARY IN CALDERA

Action	Description	Score [29]
Exfiltrated (EX)	all the sensitive are exfiltrated from host	100
Escalated (ES)	host escalated	1
Enumerated (EN)	local host discovery	5
probed Accounts (PA)	The probed to discover local admin in the network	2
Exploited(E)	host attempted to exploit,	1
Lateral Movement (LM)	move the host laterally	4
Dump creds(DC)	host's credentials are dumped	1

The score is used to calculate the adversary's probabilistic in ordering the different techniques used by the adversary's purposes and based on skills, knowledge etc.,

TABLE VII. ACTIONS ON DIFFERENT ATTACK PATTERN

Action 1	Action 2	Action 3	Action 4	Action 5
EN	E	PA	LM	PA
EX	PA	DC	EN	EX
ES	EN	E	PA	DC
DC	EX	LM	ES	E
LM	ES	ES	E	ES
E	LM	EX	DC	EN

The mean and the std deviation are calculated to identify the variances between the actions of the adversaries in listing the profile to secure the assets of the organization. From fig7,it is observed that the TTP's are vary from adversary and also the practices of tactics and techniques would vary. Thus, theadversary always dynamically changes their behaviour to be long persistence till the system gets compromise and exfiltrate the data.

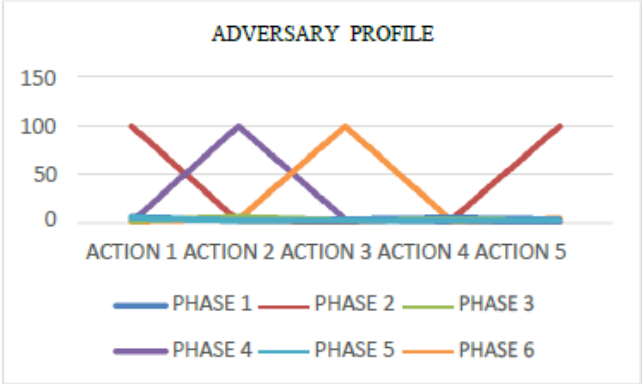

Fig. 7.Creating the adversarial Profile

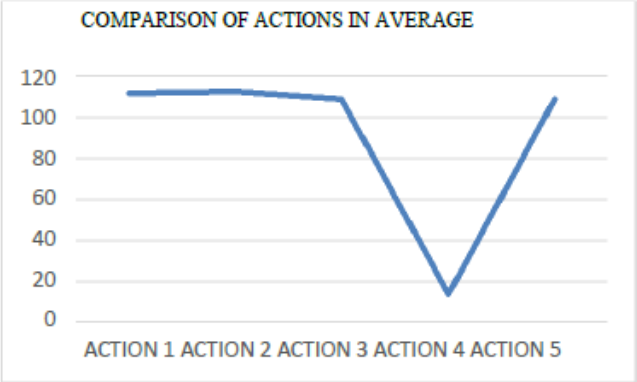

Fig. 8.Average of adversarial actions

From fig 8. TTP used by the adversary may be similar and some may entirely change the attack pattern based on their large amount of time consuming effort is trialled in develop an different attack pattern .Noticing the graph , it is clearly observed that action 4 is drastically low due to the Exfiltration is not included in the pattern,so it is considered to be easiest one when comapare with other actions which has included the exfiltration in the attack pattern due to its higher value of effort .

VI. CONCLUSION

The adversarial emulator is used to identify the assets of the organization and to protect from the adversaries. By planning the phases of the APT attacks, adversaries' profile is created using caldera. The adversary emulators can be used to find the impacts of the actions of the adversary in order to protect the assets. As the adversary's profiles are created and evaluated on TTP's to be resilient for safe-to-fail operations. Thus, the caldera emulates the world of adversaries to enlighten the defender's mechanism.

REFERENCES

1. Yang, Lu-Xing, Pengdeng Li, Xiaofan Yang, Luosheng Wen, Yingbo Wu, and Yuan Yan Tang. "Security evaluation of cyber networks under advanced persistent threats." arXiv preprint arXiv:1707.03611 (2017).
2. Redondo-Hernández, Alberto, Aitor Couce-Vieira, and Siv Hilde Houmb. "Detection of Advanced Persistent Threats Using System and Attack Intelligence." (2015): 90-94.
3. Cho, J. H., S. H. O. U. H. U. A. I. Xu, P. Hurley, M. A. T. T. H. E. W. Mackay, T. R. E. V. O. R. Benjamin, and MARK BEAUMONT. "STRAM: Measuring the trustworthiness of computer-based systems." ACM Computing Surveys (under review). Google Scholar (2017).
4. Ramos, Alex, Marcella Lazar, Raimir Holanda Filho, and Joel JPC Rodrigues. "Model-Based Quantitative Network Security Metrics: A Survey." IEEE Communications Surveys & Tutorials 19, no. 4 (2017): 2704-2734.
5. Su, Yunfei, Mengjun Lib, Chaojing Tang, and Rongjun Shen. "A Framework of APT Detection Based on Dynamic Analysis." (2016).
6. Rot, Artur, and Boguslaw Olszewski. "Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection." In In 2017 Federated Conference on Computer Science and Information Systems, vol. 13, pp. 113-117. 2017.
7. John, Jeslin Thomas. "State of the Art Analysis of Defense Techniques against Advanced Persistent Threats." Future Internet (FI) and Innovative Internet Technologies and Mobile Communication (IITM) Focal Topic: Advanced Persistent Threats 63 (2017).
8. Huy Pham L., Albanese M. and W. Priest B,". A Quantitative Framework to Model Advanced Persistent Threat"s.In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications - Volume 1: SECRYPT. (2018), ISBN 978-989-758-319-3, pages 282-293. DOI: 10.5220/0006872604480459
9. Jin-Hee Cho, Shouhuai Xu, Patrick M. Hurley, Matthew Mackay, Trevor Benjamin, Mark Beaumont. "STRAM", ACM Computing Surveys, 2019
10. Google dongs(2019) on PenTestIT available on http://pentestit.com/adversary-emulation-tools-list/
11. Azeria-labs 2017.Intro to APT28 & APT30 (2017). https://azeria-labs.com/intro-to-apt28-apt30/
12. Andrew Smith (2017) Cambridge Centre for Risk Studies 2017 Risk Summit Available on https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/170622-slides-smith.pdf
13. DavidJBianco(2018)Enterprise Detection & Response webpage on The Pyramid of Pain on http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
14. An automated adversary emulation system on https://github.com/mitre/caldera(2018)
15. Noor, Umara, Zahid Anwar, Asad Waqar Malik, Sharifullah Khan, and Shahzad Saleem. "A machine learning framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories." Future Generation Computer Systems 95 (2019): 467-487.
16. Online browser and desktop app, neo4j, http://localhost:7474/browser/Bloodhound/BloodHoundExample DB graphdb
17. Noor, Umara, Zahid Anwar, and Zahid Rashid. "An Association Rule Mining-Based Framework for Profiling Regularities in Tactics Techniques and Procedures of Cyber Threat Actors." In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), pp. 1-6. IEEE, 2018.
18. Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. (2017). Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence. Journal of Management Information . Systems, 34(4), 1023–1053. doi:10.1080/07421222.2017.1394049
19. Benjamin, V., and Chen, H. Securing cyberspace: Identifying key actors in cybercriminal communities. In Proceedings of the IEEE Joint Intelligence and Security Informatics Conference. Washington, DC: IEEE, 2012, pp. 24–29. 9.
20. Benjamin, V.; Zhang, B.; Nunamaker, J.F.; and Chen, H. Examining hacker participation length in cybercriminal Internet-relay-chat communities. Journal of Management Information Systems, 33, 2 (2016), 482–510. 10.
21. Benjamin, V.; Li, W.; Holt, T.; and Chen, H. Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops. In IEEE International Conference on Intelligence and Security Informatics. Baltimore, MD: IEEE, 2015, pp. 85–90.
22. Holt, T.J. Examining the forces shaping cybercrime markets online. Social Science Computer Review, 31, 2 (2013), 165–177(DATASET)
23. Qamar, Sara, Zahid Anwar, Mohammad Ashiqur Rahman, Ehab Al-Shaer, and Bei-Tseng Chu. "Data-driven analytics for cyber-threat intelligence and information sharing." Computers & Security 67 (2017): 35-58.
24. Noor, Umara, Zahid Anwar, Tehmina Amjad, and Kim-Kwang Raymond Choo. "A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise." Future Generation Computer Systems 96 (2019): 227-242.
25. J. Radianti and J.J. Gonzalez, "A preliminary model of the vulnerability black market," Society, 2007.
26. Dube, Thomas, Richard Raines, Bert Peterson, Kenneth Bauer, and Steven Rogers. "An investigation of malware type classification." In International Conference on Cyber Warfare and Security, p. 398. Academic Conferences International Limited, 2010.
27. Fachkha, Claude, and Mourad Debbabi. "Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization." IEEE Communications Surveys & Tutorials 18, no. 2 (2015): 1197-1227.
28. Bou-Harb, Elias, Mourad Debbabi, and Chadi Assi. "A novel cyber security capability: Inferring Internet-scale infections by correlating malware and probing activities." Computer Networks 94 (2016): 327-343.
29. Lemay, Antoine, Joan Calvet, François Menet, and José M. Fernandez. "Survey of publicly available reports on advanced persistent threat actors." Computers & Security 72 (2018): 26-59.