IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 2, 2020, accepted February 22, 2021, date of publication March 17, 2021, date of current version March 23, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3066289

SBI Model for the Detection of Advanced Persistent Threat Based on Strange Behavior of Using Credential Dumping Technique

NACHAAT MOHAMED, (Member, IEEE), AND BAHARI BELATON
School of Computer Sciences, Universiti Sains Malaysia, Penang 11800, Malaysia
Corresponding author: Nachaat Mohamed (eng.cne1@gmail.com)

This work was supported in part by the USM Research University Grant (RU) under Grant 1001/PKOMP/8014018.

ABSTRACT This study investigated the shift from the manual approach of processing data to the digitized method making organizational data prone to attack by cybercriminals. The latest threat Advanced Persistent Threats (APT) was originated by the United States Air Force in 2006 by Colonel Greg Rattray. APT is constantly ravaging industries and governments, which causes severe damages including data loss, espionage, sabotage, leak, or forceful pay of ransom money to the attackers. This study introduces a new model built on Adversarial Tactics Techniques and Common Knowledge (ATT&CK) matrix for detecting APT attack. This is to identify the APT on the first potential victim when the attackers use credential dumping technique. Strange Behavior Inspection Model incorporating several models investigates and monitors APT behavioral features in the CPU, RAM, windows registry, and file systems proposed to detect APT Attack at the first potential victim machine. The Strange Behavior Inspection (SBI) Model proposed in this paper is designed to detect the attack before being developed to more advanced phases. The results of this study are presented at four levels:1- random access memory, 2-central processing unit, 3- windows registry, and 4- file systems. This study proposes a unique model as evidence to detect APT attacks before any other techniques are used. The proposed model reduces the detection time from nine-months to 2.7 minutes.

INDEX TERMS Attacker, APT, exploit, ATT&CK, dump, Mimikatz and credential dumping.

I. INTRODUCTION

The evolution of the Internet and computer networks has initiated new and sophisticated types of attacks called the Advanced Persistent Threat (APT). The term APT was formulated by Colonel Greg Rattray serving in the United States Air Force in 2006 [1]. APT attacks are furtive and orchestrated attacks targeting organizations and governments to exfiltrate confidential data [2], [3]. The APT attackers, without being detected, concede in the network for a long time to steal data and critical information [4]. Such attacks leverage multiple vectors and entry points to navigate around defenses to breach the network in minutes and evade the radar of traditional security measures and detection for months. APT attackers are well-funded and highly skilled in hacking working for governments, military units, intelligent units, or other highly organized groups [4]. These groups work methodically to gain access to the target (like military and economic value), and they have the capability to take advantage of zero-day vulnerabilities to perform their attacks. There is a wide range of techniques used to exploit the earmarked organization. This includes deception to download materials, and includes the use of tools such as malware, SQL injection, spam, spyware, phishing, etc. [5]. The recent years have witnessed a drastic increase in the number and the scale of APT attacks that exploit loopholes and vulnerabilities to control businesses to their advantage. Utilization of social engineering techniques is an approach that exemplifies APT attacks that trick people to violate standard security procedures or deceive employees of the targeted organization to violate or abuse legitimate access rights. While leveraging ghost net techniques to stay for a long period inside organization's infrastructure. This, therefore, creates a scenario of an insecure environment for many online organizations [2]–[6]. Typical cybercrimes and their APT attack activities are described in Figure 1.1 (Source: emagcomsecurity.wordpress.com).

Figure 1.1 demonstrates how an APT attacker employs a complex mixture of attack methods by targeting multiple

The associate editor coordinating the review of this manuscript and approving it for publication was Yassine Maleh.

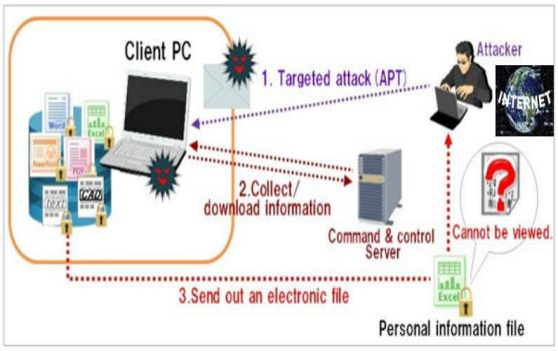

FIGURE 1. A Conventional APT attack cycle showing APT attacker sending a message to his victim, and waiting for a response (action), hence APT attacker will be able to get RDP at target machine, then install credential dumping applications to reach the key servers over infrastructure and exfiltrate the data.

vulnerabilities within an organization. The operation may identify primary people of the victim's organization by carrying out multiple techniques as follows:

- Social engineering attacks such as telephone-based attack.
- Internet malware such as infection like phishing emails to install Remote Access Tools (RAT).
- Physical malware such as using infected USB sticks and memory cards.
- External exploitation through injecting customized code into privileged hosts and exploitation of mass vulnerability [7].

Business organizations are not the only target of APT attacks. Most government's high-ranking offices are on the radar of the APT attacker's surveillance [8]. After successfully gaining access into the network, the attacker installs malware on the computer of the victim. They then scale up the search to find other vulnerable hosts to pivot and hide their presence to ensure the highest privilege to reach their goal [3]. The attackers grants themselves administrative rights to remotely control the network infrastructure to observe and steal sensitive data. The Command and Control (C&C) as a separate channel is used to execute the command and infiltrate the breached sensitive data. The attackers continue to write and rewrite codes using several savvy techniques to maintain access to the network and evade detection while carrying out malicious actions [9]. Unlike other classes of attacks, the APT attacker uses modern patterns to accomplish their agenda. The attack trails its target constantly for a long period of time, and steadily penetrate the network. Numerous attack cases have shown that this kind of attacks are stealthy and extends over an exceptionally long period until the victim or network administrator detects the malicious activities. Penetration and insertion into the network takes ten-month period to twenty-eight-month period [10]. The implication of an APT attack is a huge loss in terms of data and monetary loss, which may lead to bankruptcy of a business. APT is increasingly recognized as a seriously worldwide concern that affects all sectors in the target countries, banks, health, education, army, water, and electricity. For these reasons, the problem has attracted the security community to device novel solutions in a bid to solve the APT problem. This is because a country can be erased/damaged electronically by being involved in wars and conflicts. Some of the attacks against institutions around the world use machine learning (ML) algorithms, and zero-day vulnerability to attack targets [3], [4]. With the innovative tactics, techniques and procedures (TTPs) used by threat actors, cyber-attacks are becoming major risks to any government or multinational / national organization [53]. In this paper, an SBI model that proposes ''a threat intelligence'' method which derive malicious APT behaviour from credential dumping techniques. The model scrutinizes and gathers evidence from crucial host resources such as RAM, CPU, Window Registry and File System. Equipped with these evidences, the model is able to detect APT attack at first potential victim. Therefore, the goals of this paper are to address limitations in existing solutions which realize on signature based or known attacks to detect APT attacks. One of the most important characteristics of an APT attack is that it is not known signature, rather it exhibits suspicious behavior in credential dumping. Therefore, APT attacks are hard to detect. Built based on this observation, the proposed SBI solution, therefore, focuses on the weakest points of APT lifecycle which is the occurrence of suspicious behavior found in credential dumping. SBI model is unique as it updates it rules and parameters automatically from the credential dumping data extracted from ongoing attacks. This, thus, makes this model completely unique and different from existing solutions which also prepare it for practical solutions.

II. BACKGROUND STUDIES

This part of the paper presents some of the terms used in the context, and which are used during the implementation of SBI model to detect APT groups in credential dumping technique.

Credential Dumping: is a technique used by APT groups to obtaining the users, passwords, and tickets from the victim machine. These credentials used to give APT high level of privileges and perform Lateral Movement [4].

Moving Target Defense (MTD): it is an approach to control alter over different framework measurements to raise instability and clear difficulty for attackers, decrease their window of opportunity and increment the costs of their testing and assault endeavors.

Spear phishing: Is an e-mail or electronic communications trick focusing on a particular person, organization, or trade. Although used to take information for malevolent purposes, cybercriminals may install malware on a focused-on user's computer.

Adversary: This portrays an individual such as a hacker, who has aptitudes in programming, organizing and consistent investigation. The adversary has illegal access to websites and systems and may take data to shakedown individuals or to brag.

ATT&CK: it is MITRE Adversarial Tactics, Techniques & Common Knowledge. It is an adversary model; pretty much like Lockheed Martin Cyber Kill Chain [4]. It is clearer and more detailed to describe the real behavior of APT tactic by tactic and technique by technique,

Vulnerability: it is a weakness in the computer system which the adversary can use to get an access and control the system. It refers to the inability of a system, application, or database to withstand the effects of a hostile environment.

Gain Access: it is about the successful use of one or more technique under initial access tactic in MITRE ATT&CK to set a foothold inside target infrastructure.

Whitelisting: This is a security procedure to restrict the use of the systems from running software and it is cleared for safe execution.

III. RELATED WORK

Advanced Persistent Threats (APTs) are classified as a recent type of cybersecurity threat run by highly skilled and well-resourced adversaries that targets precise information in governments and high-profile organizations, mostly in a long-term campaign entailing different phases [8]. APT is a dangerous form of attack launched through the Internet from a computer in a remote environment where the attacker exists to target computer network. The targeted computer network belongs to either the government(s), or particular persons [4]. APT attacks are often successful because of their operational strategies different from the traditional attack, which thus bypasses state-of-the-art traditional detection measures. There is a disparity between APT and the traditional type of attack. APTs usually target a specific organization for a specific purpose. Recent cases of APT have showed that the attackers exploit a zero-day vulnerability of software, modify, and obfuscate organizational source codes in the infrastructure to remain undetected by the traditional countermeasures. For instance, measures where signature-based endpoints protected by firewalls, network intrusion protection system (NIPS), intrusion detection system (NIDS), and anti-virus would still be unable to detect APT attacks. The drive-by compromise technique is part of the Adversarial Tactics Techniques and Common Knowledge (ATT&CK) Model utilized as a basis in this study. In this scenario, the adversary takes advantage of the potential victim by exploring the websites allowed by the victim's organization and by checking the websites allowed and visited daily by the organization [11], [12]. In their latest study in 2018/2019, Ponemon Institute and IBM [13] reported that the cost per data breach was 2.53 million dollars in 2018. This increased to 3.9 million dollars in 2019. The cost per record was 125 dollars in 2018 and increased to 150 dollars in 2019 [13]. The average time to detect one APT attack, taking previously six months, has become nine months in 2019 [13]. In addition, APTs are typically slow and habitually spread over a long time. Consequently, APTs fall outside the limited detection and correlation window of traditional systems [14], [9].

TABLE 1. Comparison of traditional attacks and APT attacks.

Description	Conventional Attacks	APT Attacks
Attacker	Mostly by an individual	Mostly by group, the attack is sophisticated, highly organized, deterministic, and well-coordinated
Target	Unspecified, mostly individual systems	Noted organizations, government agencies, commercial enterprises, and military
Purpose	Mostly for financial benefits, demonstrating capabilities	Competitive gains, superiority control, strategic benefits
Approach	Single-run, smash and grab tactics, short period of invasion	Repeated or persistent attempts, hidden, moving slow and low, adapts to resist kind of defenses, a long period of invasion

ATT&CK: Adversarial tactics techniques and common knowledge matrix developed by MITRE describe the real behavior of APTs starting from reconnaissance passing through Initial Access, Execution, Persistence, Privilege Escalation, Defines Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control down to exfiltration and impact. This matrix consists of 12 tactics and more than a hundred techniques that summarize this matrix in four stages, namely: reconnaissance, initial access, credential access, and exfiltration [4]–[15]. This research provides a unique model to detect APT by applying credential access tactics, specifically in credential dumping technique.

A. HONEYPOT AND HONEYNET STRATEGIES

The degree of attack employed to carry out the attacks is one of the characteristics of APT attacks. [2]. The widespread malware and mode of attack are difficult for most organizations/defenders to handle. Often, a proactive measure such as a deception technology can help battle against the unexpected and unknown attacks [9]. In defense methodology, defenders may deceive attackers by creating baits in a decoy form which resembles the production environments being not truly part of the organization's production setting. Access monitoring to such honeypots and honeynets can assist organizations in detecting the APT attack [2].

B. MOVING TARGET DEFENSE

In [9]–[21] researches enumerated the significance of reconnaissance defences. This includes deception and movement. The researchers explained that moving target defenses is operated by constantly changing the attack surface. This does not allow attackers to make static and long-time assumptions about the network, which thus counters the reconnaissance

phase of invasion. An example of moving target defense (MTD) is the network shuffling, which remaps targets' addresses in an attempt to render scanning useless [17]. Further discussed the deception defenses involving honeypots that could be used to effectively deceive attackers achieving reconnaissance on potential targets in a network [27].

Hence, the authors propose probabilistic models that provide the benefits and costs related to reconnaissance defenses. This may thus assist in understanding the circumstances of how the models can be most effective [17]. The authors evaluated their models using two numbers of attacker scenarios, that is, foothold design and minimum to win. The study concludes that a small number of honeypots could enable significant cyber defense in different situations. This could thus be better than defense by movement in the evaluated scenarios, though having both can give the best reconnaissance defense performance. Built on the extant literature, there are some highlighted moving target defense techniques against APT's. These techniques are used by most organizations. Some of these MTDs are presented in Table 2.

TABLE 2. Moving target defense.

Reference	Details	MTD Strategy
[20]	SDN-based solutions for moving target defense. network and host MTD	OS hiding, Network reconnaissance protection.
[21]	Target movement based on attack probability	VM migration.
[22]	OpenFlow based Random host mutation	Physical IP mapping to corresponding virtual IP. Network MTD.
[23]	Fingerprint hopping method to prevent fingerprint attacks. Host MTD	Game theoretic model for fingerprint hopping.
[24]	Dynamic game based MTD for DDoS Attacks. Network MTD.	Dynamic game for flooding attacks.
[25]	Security Models for MTD. Network MTD	Effectiveness analysis for MTD countermeasures.
[26]	Dynamic MTD using multiple OS rotation. Host MTD.	Network Threat based OS rotation.
[27]	Optimal MTD strategy based on Markov Game. Application MTD.	Dynamic game, MTD Hopping.
[28]	Software Diversity and Entropy-based MTD. Application MTD.	Cost, usability analysis of software diversity.
[29]	Software Defined Stochastic Model for MTD.	High Availability and MTD Cost Modeling.
[30]	Decoy based cyber defense using Randomization. Network MTD	IP address randomization.

IV. SBI DATASET

A significant set of data collected from previous research was taken such as social media network which is not genuine [50]. The proposed dataset is evaluated using both UNICORN approach from Cornell University USA, and deep learning for frame error prediction. The adopted approach was based on DARPA dataset 1999 created/formulated by Lincoln Laboratory in Massachusetts Institute of Technology (MIT), USA. But the false positive problem in approaches depends on the use of the 1999 DARPA IDS evaluation dataset as a thorough examination which has been carried out to assess the accuracy of alerts created by Snort IDS [51], [52]. SBI dataset, composed of collection of several network available malicious and non-malicious data, has been collected during APT live attack times on three victims, with total size of 3 GB. The SBI dataset mainly uses the internal communication between hardware and software at the first target host during APT attack. The design and elements of SBI dataset are described in figure 2.

V. STRANGE BEHAVIOR INSPECTION MODEL (SBI)

With the innovative Tactics Techniques and Procedures (TTPs) used by threat actors, cyber-attacks are becoming major risks to any government or a (multi)national organization. Many organizations devour threat intelligence to increase the efficiency of the risk management method to improve the risk management metrics, and mitigation strategies. Nowadays, in many governments and organizations, Security Operation Centre (SOC) utilizes threat intelligence to improve incident detection mechanism in the various security systems of the organization. To achieve this, governments/organizations use many malware detection systems by using threat intelligence to detect malicious files entering to governments, institutions network. The SOC professionals

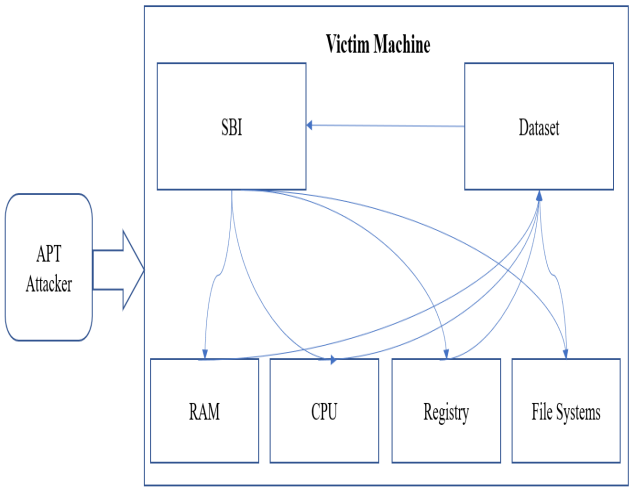

FIGURE 2. Once APT starts to achieve the credential dumping at the first potential victim, the SBI model collects the data from RAM, CPU, Registry, and File Systems.

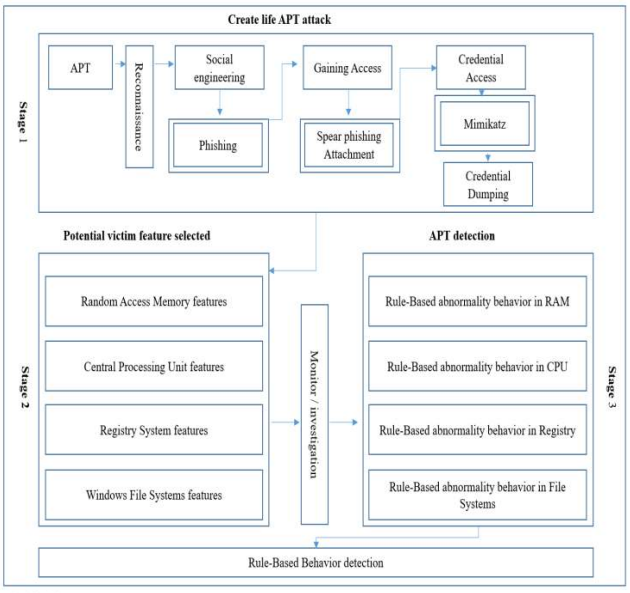

FIGURE 3. Strange Behavior Inspection Model (SBI) stage. Stage 1 create life attack based in ATT&CK. Stage 2, Potential victim features selected. Stage 3, advanced persistent threat detection at first potential victim.

use threat intelligence to categorize internal threats by categorizing information as an Indicator of Compromise (IoC), threat actors (APT), and TTPs [18], [19]. However, with SBI model, the threat intelligence is taken from malicious behavior of APT in credential dumping technique. The model will scrutinize this evidence taken from RAM, CPU, windows registry, and file systems to detect APT attack at the first potential victim. The goal of this study is to address the gap in the existing literature, based on lateral movement technique. It is obvious that the current solutions depend on signature to detect APT. One of the most important and dangerous characteristics of an APT is that they do not have signature. It only encompasses suspicious behaviors in credential dumping technique. The use of SBI model solution is based on credential dumping technique to detect APT through the only weakness point in APT lifecycle. APT attempts to dump credentials to obtain root users and passwords in a plain text through targeting file systems and registry. This is reflected on CPU utilization because of the use of credential dumping malicious applications to achieve Lateral Movement and exfiltration. Hence, APT is not able to bypass SBI model in credential dumping technique. What distinguishes SBI model is that it works independently from RAM or CPU or Windows registry or file systems. The model works from the four resources in parallel:

1- SBI model is able to work and provide detection independently and parallel based on the high-level features as instance automatic updates from the attack itself.
2- Protection against any APT groups when trying to achieve credential dumping technique.
3- Auto detection allows users and network / security administrators to know if there are any suspicious behaviors from APT at his/her machine on time.
4- Offers protection for public and private organizations with exceptionally low cost.
5- Protect entire infrastructure starting from first node (in credential dumping) before lateral movement to avoid exfiltrate toxic data and stealthy for long period.

SBI model detects APT through two stages during the APT attack. The first detection stage is the potential victim feature consisting of (RAM features, CPU features, registry features, and filesystems features). The second stage is APT detection, which consists of rule-based abnormality behavior in RAM, rule-based abnormality behavior in CPU, rule-based abnormality behavior in registry, and rule-based abnormality behavior in filesystems. These features provide a complete model against APT attacks specifically in credential dumping technique. The datasets of this research were collected during APT attack it was three gigabytes. Figure 3 show the stages of SBI model.

A. CREATE APT ATTACK

This stage aims to create a scenario for an APT attack based on ATT&CK matrix by describing the real steps of the APT attack. This is to gain access to any target. ATT&CK matrix is defined as the MITRE ATT&CK framework which is a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders in order to better classify attacks and assess an organization's risk.

B. POTENTIAL VICTIM FEATURES SELECTION

This stage illustrates the most significant features to detect APT attacks at the first point they reach. This is called the "potential victim machine." These features are extracted from the RAM, CPU, registry, and file systems. They are employed along with the credential dumping technique. These features are selected because it contains sophisticated

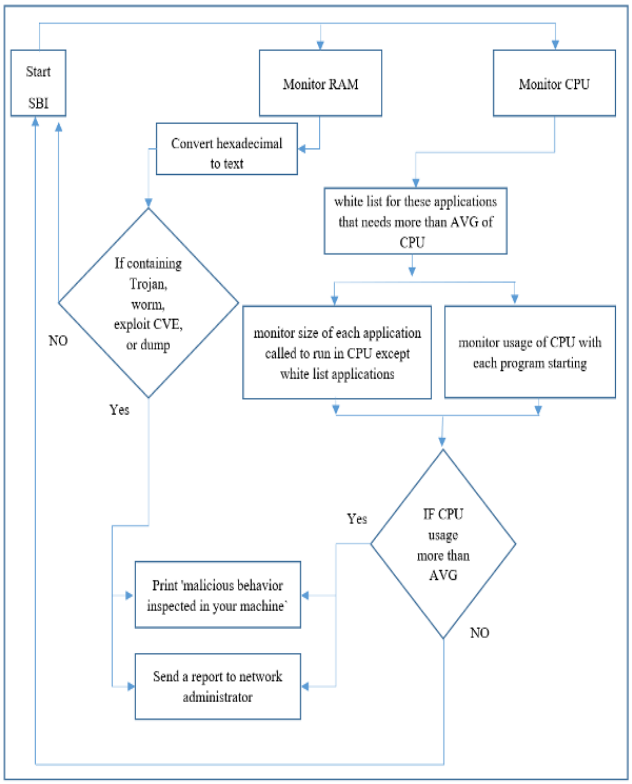

FIGURE 4. Strange Behavior Inspection (SBI) Part 1 (Resources, and Rules) at two levels RAM, and CPU.

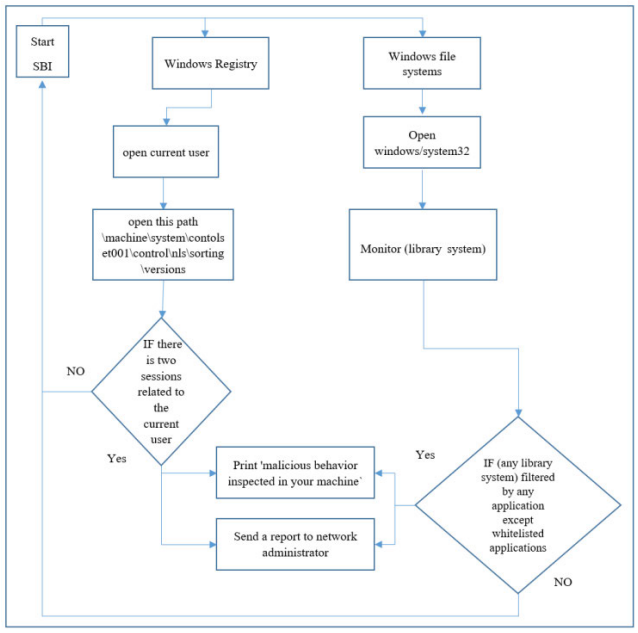

FIGURE 5. Strange Behavior Inspection (SBI) Part 2 (Resources, and Rules) at two levels Windows registry, and windows file system.

evidence during the attack time. This thus enables us to detect APT attack at the first potential victim.

C. APT DETECTION

It is essential to detect APT attack using SBI model in credential dumping technique and propose rule-based mechanism. This, thus, helps to detect the abnormality of Random-Access Memory (RAM), Central Processing Unit (CPU), system registry, and file systems.

Figure 4.0 And figure 5.0 Shows the complete design of SBI model.

D. RULE-BASED FOR DETECTING ABNORMALITY BEHAVIOR IN RAM

Rule 1 depicts the detection process of APT attacks at the victim's machine by exploring the RAM. The rule elucidates the processes of the APT attacks' detection. This means that the RAM contents are transformed from the binary to hexadecimal and then translated to textual contents. The contents, while in the process of translation, include a Trojan or anomalous behavior. In this case, the infected text should be copied using the SBI model. Therefore, a separate report is sent to the administrator.

Rule No 1

IF RAM containing input (any CVEs, malware, trojan, instance, Bundler Cluster, Meterpreter, dump command, and Exploit, except whitelisted PCs

THEN

Convert from binary to hexadecimal.

Print 'malicious behavior inspected in your machine' on user screen;

Send a report to the network administrator ('malicious behavior inspected in machine No.');

ELSE

Go to SBI, and continue to monitor RAM;

End if;

E. RULE-BASED FOR DETECTING ABNORMALITY BEHAVIOUR IN CPU

Rule 2 describes the steps necessary to detect abnormality behavior in CPU. The formula calculates the utilization in the CPU with normal applications, the average utilization of CPU stabilizes around 12.3% on a single CPU [34]. The processes referring to all are well-unknown applications requiring more than the average (AVG) of CPU utilization with 1 CPU. This excludes whitelist application. SBI model monitors the CPU for any suspicious utilization (any process that is not in the whitelist yet consuming more than average of the CPU). In the detection case, the malicious utilization state is copied via the SBI model to the dumping file, and a report is initiated to the network administrator.

Rule No 2

IF CPU usage is more than AVG to start single application **THEN**
Print ‘malicious behavior inspected in your machine‘ on user screen;
Send a report to the network administrator (‘malicious behavior inspected in machine No.’);
ELSE
Go to SBI, and Continue to monitor CPU
End if;

Rule No 3

IF windows session > 1 **THEN**
Print ’malicious behavior inspected in your machine‘ on user screen;
Send a report to the network administrator (’malicious behavior inspected in machine No.’);
ELSE
Go to SBI, and Continue to monitor registry;
End if;

F. RULE-BASED FOR DETECTING ABNORMALITY BEHAVIOUR IN REGISTRY SYSTEM

Rule 3 explains the detection process of APT inside the file registry. The registry is opened as well as the current user profile. The monitoring engine explores the following paths machine\system\contolset001\control\nls\sorting\versions; \REGISTRY\MACHINE\SYSTEM\ControlSet001 \Control\Session Manager
\REGISTRY\MACHINE\SYSTEM\ControlSet001 \Control\Session Manager

In this path, if there are two sessions for the same user, then there is a malicious behavior, and the SBI model intervenes by copying to the dump file and by reporting the incident to the network administrator.

G. RULE-BASED FOR DETECTING ABNORMALITY BEHAVIOUR IN FILE SYSTEMS

Rule No 4

IF (any library system) filtered by any application except whitelisted applications **THEN**
Print ’malicious behavior inspected in your machine‘ on user screen;
Send a report to the network administrator (’malicious behavior inspected in machine NO.’);
ELSE
Go to SBI and Continue to monitor file system.
End if;

Rule 4 the library system are not allowed to be filtered by any unlisted application except these whitelists are prepared in advance. In the case of detecting filtration to the file system, the dump file is copied via the SBI, and a report sent to the network/security administrator.

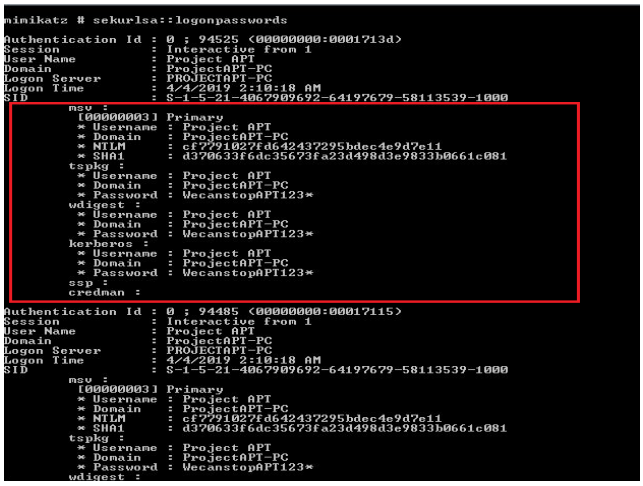

FIGURE 6. Results before using SBI Model against APT show that they are able to get the whole users, and passwords in plain text.

VI. WHY ARE APT FILTRATING THE DLL FILES?

This paper investigates the whole DLL files appeared during APT experiment attack. This study finds that there is a significant relationship between these DLL files in table 3, worked on in this study, and Common Vulnerabilities and Exposures (CVE) in table 3. This allows APT to execute arbitrary code on the potential victim. Meanwhile, other files give APT capability to edit and overwrite in overly critical libraries.

VII. DEVELOPMENT AND IMPLEMENTATION

The proposed model supports a set of unique indicators to detect APT groups in the first potential victim machine. This is based on investigating features of resources in that machine. The general stages of the proposed approach are comprised of (i) creating real-life APT attack, (ii) potential victim machine feature extracted, and (iii) potential victim rule-based APT detection. The stages of implementation approach are executed when the APT attacker tries to achieve initial access tactic. This, which thus helps achieve credential dumping technique under credential access tactic. This paper provides/proposes a real APT attack from initial access tactic passing through credential access tactic and reaching to credential dumping technique. This study employs Kali Linux distribution [4] which contains more than 700 applications for hacking and malicious credential dumping application ‘‘Mimikats’’, used by APT groups.

A. BEFORE IMPLEMENT SBI MODEL

After running live attack(s) and using Mimikatz on the victim and before installing SBI model. The results are demonstrated in figure 6, and other essential information is provided i.e., the super user, password, and NTLM in plain text. Password was fire password (**WecanstopAPT123***)).

B. AFTER IMPLEMENT SBI MODEL

The SBI model was installed on three machines in the infrastructure. The accuracy detection for each victim was 99.8%.

TABLE 3. Provide the relation between DLL files and CVEs.

DLL File	Description	CVE that have relation
GDI32.dll	Functions for the Windows GDI	CVE-2006-4071 CVE-2005-4560 CVE-2005-0803 CVE-2005-2124,
kernel32.dll	Windows kernel module	CVE-2007-4528 CVE-2007-5145
KERNELBASE .dll	Windows NT BASE API Client DLL	CVE-2003-0109
ADVAPI32.dll	Dynamic link library	CVE-2017-11742
CRYPT32.dll	Module that implements many of the Certificate and Cryptographic Messaging	CVE-2003-0818
CRYPTBASE.dll	Base cryptographic API DLL	CVE-2017-7327
cryptdll.dll	Module associated with Cryptography Manager	
MSASN1.dll	Abbreviation for Dynamic Link Library	CVE-2003-0818 CVE-2005-1935
NETAPL32.dll	module that contains the Windows NET API used by applications to access a Microsoft network	CVE-2003-0938 CVE-2008-4250
ntdll.dll	File that contains NT kernel functions	CVE-2003-0109 CVE-2006-2334 CVE-2003-1246 CVE-2006-1510 CVE-2007-5145
ole32.dll	Library which contains core OLE functions	CVE-2006-6659 CVE-2006-1540 CVE-2007-1347
profapi.dll	Shared dynamic link library that stores program c	CVE-2017-7327
RPCRT4.dll	Remote Procedure Call, used by Windows applications for	CVE-2007-2228

TABLE 3. *(Continued.)* Provide the relation between DLL files and CVEs.

	network and Internet communication	
SAMLIB.dll	Library used for the Security Authority Manager API	CVE-2018-6766
secu32.dll	Library which contains Windows Security functions.	CVE-2016-4349, CVE-2017-11157, CVE-2017-11159
SHLWAPI.dll	Library which contains functions for UNC and URL paths, registry entries, and color setting	CVE-2012-0454
SSPICLI.DLL	Related to problems with Windows Dynamic Link Library	CVE-2016-5821
USER32.dll	Module that contains Windows API functions related the Windows user interface	CVE-2003-0659 CVE-2005-1793
USERENV.dll	Module that contains application programming interface (API) functions to create and manage user profiles	CVE-2010-3129 CVE-2016-5821
USP10.dll	File that runs Uninscribed services	CVE-2013-3181 CVE-2014-1817 CVE-2010-2738 CVE-2016-1281
Secur32.dll	Library which contains Windows Security functions	CVE-2016-4349 CVE-2017-11157 CVE-2017-11159
SHELL32.dll	Library which contains Windows Shell API functions	CVE-2007-6753 CVE-2007-3896 CVE-2003-0503 CVE-2005-2127 CVE-2005-1990

TABLE 3. *(Continued.)* **Provide the relation between DLL files and CVEs.**

VERSION.dll	Module that contains application programming interface (API)	CVE-2017-1000010 CVE-2017-0038 CVE-2003-1048 CVE-2019-7364
WINSTA.dll	An executable file	CVE-2018-6765
OLEAUT32.dll	Stands for "Object Linking and Embedding Automation	CVE-2014-6332, CVE-2002-1444
INTRUST.dll	Is indicates to an attack and attempt against a File Overwrite vulnerability in Quest InTrust.	CVE-2012-5896 CVE-2012-5897
SAMLIB.dll	Public Library used for the Security Power Manager API	CVE-2018-6766

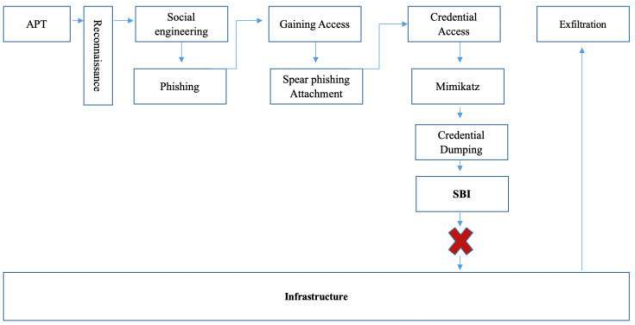

FIGURE 7. **SBI Model able to detect APT in Credential Dumping and avoid exfiltration techniques.**

SBI model should be installed at/on every single windows operating system to detect APT in the target infrastructure. The reason why this paper provides a solution in credential dumping technique is because of the credential dumping technique is a fragile point in APT lifecycle. There is a suspicious running behavior merely in this technique. This paper answers this question as illustrated in figure 7. The study employs the design accomplish attack mission with SBI model to avoid the significant problem of exfiltration, and other issues of APT like stealthy, espionage, long period attack, and sabotage. This becomes after APT achieves credential dumping technique without detections and reach to lateral movement, hence exfiltration.

VIII. ANALYSIS AND RESULTS

The previous sections discusses the design of the proposed model SBI. This section reports and analyzes the experimental results obtained by the proposed model. The proposed SBI model is the outcome of this research, the aim of which is to devise a model to detect APT attackers in the first potential victim. This paper presents a different proposition to the previous and current solutions. Hence, the results of the APT investigation could be unique.

A. TERRESTRIAL OBSERVATIONS TEST SCENARIO

These terrestrial observations test scenarios that aim to evaluate the ability of the proposed SBI model to detect APT attacks at the first potential victim in the credential dumping technique. The evaluation mainly focuses on the calculation of the detection accuracy and false positive rate of SBI model. The scenarios provided are used to evaluate the proposed model using the dataset that is described in the previous section.

B. TERRESTRIAL OBSERVATIONS REAL TIME DETECTION ANALYSIS SCENARIO

The provided model SBI gathers the data from four resources RAM, CPU, windows registry, and file systems. The access period to read or write any specific byte is autonomous of whereabouts in the memory that byte is, which is approximately 50 nanoseconds. This is broadly equal with the speed at which the central processing unit requires to access these data. This will be much lesser, but in other resources, such as 5 nanoseconds from CPU cache [31], [32]. The total data gathered from the registry, file system, and CBU are 737 bytes, and the rest of the three Giga was from RAM. The RAM is 1000 times faster read rate compared with hard disk drive HDD [33]. This means it takes 50 x 1000 = 50,000 NS to read one byte from HDD, accordingly, the required time to read 737 bytes is 737 x 50,000 = 36,850,000 NS. The equation 1 describes the total nanosecond of hard disk which uses the abbreviation (TNSHD), bytes of hard disk which uses the abbreviation (HB), and hard disk nanosecond which uses the abbreviation (HDNS).

$$\text{TNSHD} = \sum \text{hb} \times \text{hdns} \tag{1}$$

Based on this time (50 nanoseconds) to read/write a specific byte from RAM [31], [32]. This paper suggests the real-time required to detect APT attacks at first potential victim. Gigabyte uses the abbreviation (GB), byte uses the abbreviation (B), nanosecond uses the abbreviation (NS), and second which uses the abbreviation (S). One gigabyte = 1024 × 1024 × 1024 = 1,073,741,824 byte. Based on the dataset mentioned in the previous sections, 3 gigabytes, = 1,073,741,824 × 3 – 737 = 3,221,224,735 bytes. The equation of gigabit is shown in Eq.2.

$$\text{BG} = \sum (1024 \times 1024 \times 1024) \tag{2}$$

One second = 1,000,000,000 nanosecond. As shown in the

$$\text{S} = \sum 1\text{E} + 9 \tag{3}$$

The total nanosecond = 3,221,224,735 byte x 50 nanosecond = 161,061,236,750 nanosecond. As shown in the equation of

TABLE 4. Measure Unit & Detection Time.

Measure Units & Resources	Results & Detection time
Gigabyte	109 bits
Byte	8 bits
Second	1E+9 NS
Total bytes of HDD	737
Total nanoseconds of HDD	36,850,000
Total bytes of RAM	3,221,224,735
Total nanoseconds of RAM	161,061,236,750
Detection Time	2.7 Minutes

total nanosecond Eq. 4.

$$\mathrm{NS} = \sum(\mathrm{gb} \times 50) \tag{4}$$

The total no of seconds to detect APT will be 161,061,236,750 + 36,850,000 / 1,000,000,000 /60 = 2.7 Minutes to detect APT at first potential victim in credential dumping techniques. As shown in the equation of real time to detect APT Eq. 5.

$$\mathrm{DT} = \sum(\mathrm{ns} + \mathrm{tnshd})/(1\mathrm{E} + 9)/60) \tag{5}$$

This section provides the real time taken by SBI model to detect APT groups at the first potential victim, The Measure Unit & Detection Time have been filled out as shown in table 4.

C. EVALUATION METRICS

The ability of SBI model to detect APT attacks at the first potential victim is evaluated using accuracy detection measurements which are typically used in the other studies to clarify experiments [44]. This measurement depends on a true positive (TP, the number of malicious behaviour correctly classified as malicious), true negative (TN, the number of normal behaviour correctly classified as normal), false positive (FP, the number of normal behaviour wrongly classified as a malicious), false negative (FN, the number of malicious behaviour wrongly classified as a normal. The main goal of this measurement and what it depends on is to get detection accuracy (DA) as shown in table 5.

To evaluate the accuracy of the proposed model, this research applies the rules of APT detection at the first potential victim based on the malicious behavior of using credential dumping techniques. It uses the results from these rules used to validate detection accuracy measured by (Eq 6 to Eq)10.

$$\mathrm{DA} = \sum(\mathrm{TP} + \mathrm{TN})/(\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}) \tag{6}$$

TABLE 5. Evaluation Metrics.

	Malicious Behaviour	Normal Behaviour
Malicious Behaviour	True positive	False positive
Normal Behaviour	False negative	True negative

$$\mathrm{FP} = \sum \mathrm{FP}/(\mathrm{TN} + \mathrm{FP}) \tag{7}$$

$$\mathrm{TP} = \sum \mathrm{TP}/(\mathrm{FN} + \mathrm{TP}) \tag{8}$$

$$\mathrm{TN} = \sum \mathrm{TN}/(\mathrm{FP} + \mathrm{TN}) \tag{9}$$

$$\mathrm{FN} = \sum \mathrm{FN}/(\mathrm{TP} + \mathrm{FN}) \tag{10}$$

D. TERRESTRIAL OBSERVATIONS (ACCURACY)

The detection accuracy scenario evaluates the detection accuracy of the proposed Strange Behavior Inspection Model over the SBI dataset. Based on [31]–[33] the access period to read or write any specific byte is autonomous of whereabouts in the memory that byte is, and is approximately 50 nanoseconds, and 50,000 ns to read from HDD. The real detection time is described in details in section (terrestrial observations detection accuracy scenario). This section presents the accuracy detection, false positive, false negative, and true positive based on using credential dumping malicious application (Mimikatz) employed by APT28, APT32, Axiom, Carbanak, HOMEFRY, Leviathan, OnionDuke, PinchDuke, Poseidon Group, Revenge RAT, Sowbug, Suckfly, Trojan.Karagany groups. Based on the malicious behavior of using credential dumping technique by APT attacker, this research proposes the accuracy detection.

Conversely, before all of these, why based on malicious behavior, and not based on signature? Malicious behavior refers to unauthorized changes by person/software to the MS Windows operating system such as registry, file systems, manage RAM apps, and user credential [45], [46]. Signature-based detection is an operation where a unique identifier is a plant about a known threat, based on the malicious signature in the application code. It should be taken into account that if APT remains below, the signature-based (happens all time), the malware is fully missing, and the whole target infrastructure remains vulnerable especially to zero-day. Regardless of how malicious code is, if signature-based applications / or hardware has not detected it before lateral movement technique, it is let through. APT can stay months, or sometimes years without any detection [35], [36].

This paper uses Receiver Operating Characteristic (ROC) to rate the accuracy detection, or sensitivity (true positive rate), and false-positive rate. In ROC the sensitivity (true positive) starts from 0,0 to 1.0 (if sensitivity = 1.0 thin true positive = 99.8% and false-positive = 0.2%). Figure 8 describes ROC [38], [39], [41]–[43].

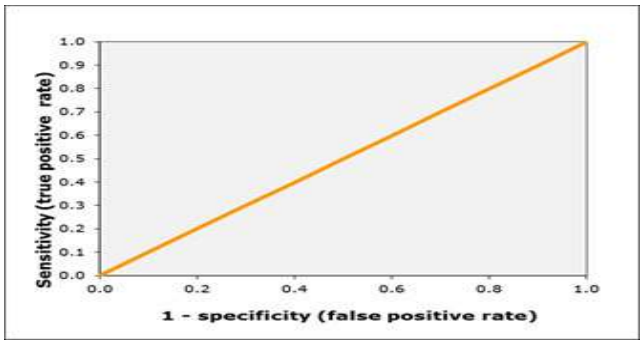

FIGURE 8. ROC Curve to measure accuracy detection and FP.

TABLE 6. Evaluation of SBI approach using provided dataset.

	172.16.140.72	172.16.140.195	172.16.140.65
Attack attempts	15	10	5
Detection attempts	15	10	5
False Positive	0.2 %	0.2 %	0.2 %
True Positive	99.8 %	99.8 %	99.8 %
Accuracy	99.8 %	99.8 %	99.8 %

Based on Receiver Operating Characteristic and SBI Dataset. APT attack targeted victim machines carried Ips 172.16.140.72, 172.16.140.195, 172.16.140.65, which started from initial access through spear-phishing (the pass rate was 99.8%). The solution proposed in this paper focuses on credential dumping technique, and thus does not target spear-phishing attack, which is a stage to be achieved before credential dumping.

Referring to [48], [36], the first stage of credential access has been accomplished. Thus, credential access tactic is to achieve through using credential dumping technique. The APT attacker targeted 3 Ips, with a total score 30 attacks, and the share of each Ip was 172.16.140.72 = 15 attacks, 172.16.140.195 = 10 attacks, and 172.16.140.65 = 5 attacks. In the frequent process of running credential dumbing malicious application, SBI model was able to detect the malicious behavior in four resources RAM, CPU, registry, and file systems. The result is described in Table 6.

E. RAM ABNORMALITY BEHAVIOR TEST SCENARIO

CVE-2017-1188: Microsoft office vulnerabilities are used to distribute malware apps to creating backdoor. MS Office uses Microsoft Equation Editor, which is one of the most important components of Microsoft Office. Microsoft Equation Editor contains a stack buffer overflow vulnerability that enables the attacker to execute remote code execution on a target / vulnerable system. The Microsoft Equation Editor was compiled in November 2000. Without any further improvement or enhancement, it is solely used in all Microsoft Office [49]. Some of the solutions designed to help us is Microsoft

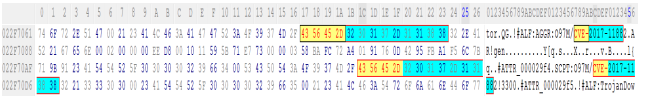

FIGURE 9. SBI Model exposed APT while attempting to exploit the CVE-2017-1188 vulnerability.

Equation Editor that contains a stack buffer overflow vulnerability, which can permit an inaccessible, unauthenticated assailant to execute subjective code on a defenseless framework. Equation editor is a component/feature in Microsoft Office. It is an out-of-process COM server that is facilitated by eqnedt32.exe. Memory corruption vulnerabilities in modern solution are often mitigated by exploit protections, such as DEP and ASLR. However, APT attackers are still able to bypass these protection methods. Indeed, in a fully advanced patched Microsoft Office 2016 framework, the Microsoft Equation Editor needs any abuse protections. However, this lack of exploit protection gives capability to an attacker to attain code execution more effortlessly. This provides attackers with a way to decoy targets into opening specially crafted files [47]. In this section, the paper provides a random-access memory investigation and presents potential victim RAM behaviors during APT attack. The results of APT attempt to exploit the CVEs and run trojans to get a high level of privilege. Figure 9 shows the APT attacker tries to exploit CVE-2017-1188 vulnerabilities to take advantage of the potential victim.

APT attackers in our experiment tried to exploit these CVEs: CVE-2012-468, CVE-2013-0422, CVE-2014-6332, CVE-2011-1249, CVE-2013-3660, CVE-2017-0199, CVE-2015-0097, CVE-2017-0143, CVE-2015-2545, CVE-2016-1010, CVE-2012-4969, CVE-2012-4792, CVE-2010-0818, CVE-2010-2740, CVE-2010-2741, CVE-2008-5353, CVE-2010-0094, CVE-2015-1641, CVE-2017-7310, CVE-2019-0859, CVE-2012-1723, CVE-2012-5076, CVE-2015-5119, CVE-2010-3949, CVE-2017-8570, CVE-2015-6100, CVE-2015-2546, CVE-2018-4878, CVE-2011-0104, CVE-2018-8120, CVE-2019-0708, CVE-2012-1876, CVE-2016-0034, CVE-2014-0515, CVE-2019-1064, CVE-2011-0611, CVE-2013-3956, CVE-2017-14627, CVE-2012-4914, CVE-2010-3962, CVE-2011-1255, CVE-2014-4095, CVE-2015-3113, CVE-2018-15981, CVE-2011-2444, CVE-2014-1776, CVE-2015-2546, CVE-2014-4113, CVE-2013-5331, CVE-2010-3947, CVE-2014-6360, CVE-2017-0798, CVE-2014-6374, CVE-2017-0213, CVE-2012-1527, CVE-2015-1701, CVE-2011-0626, CVE-2011-1969, CVE-2013-3897, CVE-2017-0037, CVE-2015-8651, CVE-2014-0324. SBI model is designed to detect any other CVEs, malware, trojan, and dump command used by APT in credential dumping technique.

Malware or malicious application is the collective title for a few malevolent computer program variations, including ransomware, viruses, and spyware. Shorthand for malevolent program, malware regularly comprises of code created by

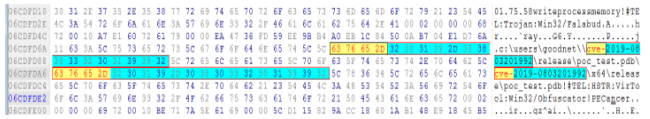

FIGURE 10. SBI Model exposed APT while attempting to exploit CVE-2019-0803 vulnerability.

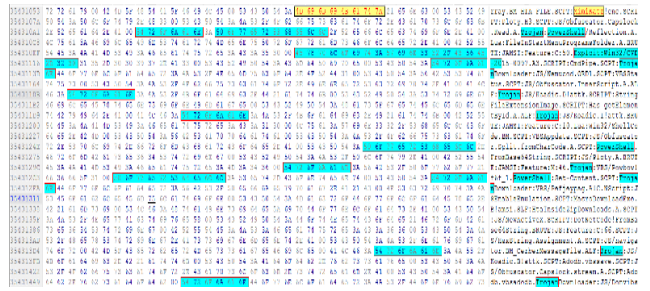

FIGURE 11. SBI Model exposed APT while attempting to run number of Trojans.

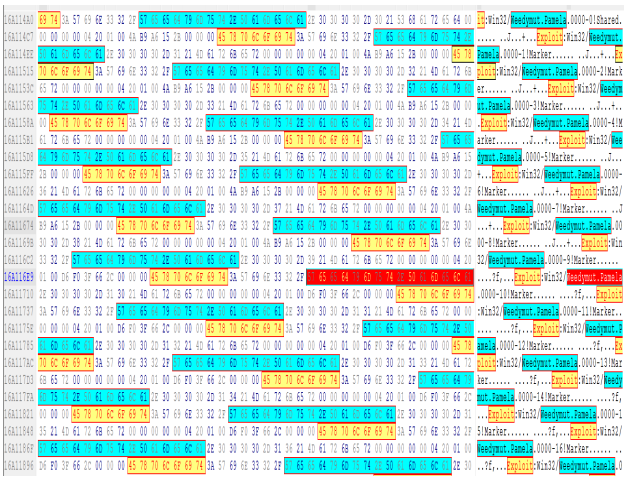

FIGURE 12. SBI Model exposed APT while attempting to take advantage at victim Machine.

cyberattacks, outlined to cause broad harm to information and frameworks or to pick up unauthorized get to a arrange. Malware is regularly conveyed within the shape of a connect or record over e-mail and requires the client to tap on the interface or open the record to execute the malware. A backdoor is about any process leading to authorized and unauthorized users to get around normal security measures without detection and to gain high level of privilege on a computer victim system, network, or any software application. Figure 11 and Figure 12 show that APT try to run number of Trojans, and open power shell command to control the victim machine [54], [55].

IX. CONCLUSION

In this paper, SBI detection model is presented to detect APT attack at the first potential victim. This reduces the detection time from 9 months to 2.7 minutes with 99.8% accuracy of detection. This paper perceivably focuses on studying the discovery process by watching the footsteps of the APT attack. It investigates the behavioral features selected from the called potential victim machine (the machine that the attack initiates its progress).This paper proposes a new model called the Strange Behavior Inspection demonstrated under the proposed model section. The proposed model detects the APT attack at the first potential victim during APT. This is done by using credential dumping technique to avoid extracting the whole users and passwords by APT attackers and prevent them to take full control at the potential victim machine. This, therefore, prevents attackers from exposing the exfiltration organizations toxic data. This paper employs the same technique (credential dumping) to detect APT attacks based on the observed malicious behavior in random access memory, central processing unit, Microsoft Windows registry, and Microsoft Windows file systems. This provides full protection against exfiltration tactic, which is regarded as a strategic benefit for advanced persistent threat groups (APT).

REFERENCES

[1] A. K. Ghazi-Tehrani, "Regulating cyber space: An examination of US-China relations," Ph.D. dissertation, Univ. California Irvine, Irvine, CA, USA, 2016.

[2] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1851–1877, 2nd Quart., 2019.

[3] Q. Zhu and S. Rass, "On multi-phase and multi-stage game-theoretic modeling of advanced persistent threats," *IEEE Access*, vol. 6, pp. 13958–13971, 2018, doi: 10.1109/ACCESS.2018.2814481.

[4] B. E. Strom, J. A. Battaglia, M. S. Kemmerer, W. Kupersanin, D. P. Miller, C. Wampler, and R. D. Wolf, "Finding cyber threats with ATT&CK-based analytics," MITRE Corp., Bedford, U.K., Tech. Rep. MTR170202, 2017.

[5] C. Xiong, T. Zhu, W. Dong, L. Ruan, R. Yang, Y. Chen, Y. Cheng, S. Cheng, and X. Chen, "CONAN: A practical real-time APT detection system with high accuracy and efficiency," *IEEE Trans. Dependable Secure Comput.*, early access, Feb. 3, 2020, doi: 10.1109/TDSC.2020.2971484.

[6] P. Gao, X. Xiao, D. Li, K. Jee, H. Chen, S. R. Kulkarni, and P. Mittal, "Querying streaming system monitoring data for enterprise system anomaly detection," in *Proc. IEEE 36th Int. Conf. Data Eng. (ICDE)*, Apr. 2020, pp. 1774–1777.

[7] H. Aldawood and G. Skinner, "Analysis and findings of social engineering industry experts explorative interviews: Perspectives on measures, tools, and solutions," *IEEE Access*, vol. 8, pp. 67321–67329, 2020.

[8] S. Siddiqui, M. S. Khan, K. Ferens, and W. Kinsner, "Detecting advanced persistent threats using fractal dimension based machine learning classification," in *Proc. ACM Int. Workshop Secur. Privacy Anal.*, Mar. 2016, pp. 64–69.

[9] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A survey of moving target defenses for network security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1909–1941, 3rd Quart., 2020.

[10] M. A. Siddiqi and N. Ghani, "Critical analysis on advanced persistent threats," *Int. J. Comput. Appl.*, vol. 141, no. 13, pp. 46–50, 2016.

[11] L. Grassi, "Mixture differential cryptanalysis: A new approach to distinguishers and attacks on round-reduced AES," *IACR Trans. Symmetric Cryptol.*, pp. 133–160, Jun. 2018.

[12] A. P. Golushko and V. G. Zhukov, "Application of advanced persistent threat Actors' techniques aor evaluating defensive countermeasures," in *Proc. IEEE Conf. Russian Young Res. Electr. Electron. Eng. (EIConRus)*, Jan. 2020, pp. 312–317.

[13] M. Parmar and A. Domingo, "On the use of cyber threat intelligence (CTI) in support of developing the commander's understanding of the adversary," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2019, pp. 1–6.
[14] Y. Zou and F. Schaub, "Beyond mandatory: Making data breach notifications useful for consumers," *IEEE Security Privacy*, vol. 17, no. 2, pp. 67–72, Mar. 2019.
[15] J. E. Rubio, R. Roman, and J. Lopez, "Integration of a threat traceability solution in the industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6575–6583, Oct. 2020.
[16] J. Halvorsen, J. Waite, and A. Hahn, "Evaluating the observability of network security monitoring strategies with TOMATO," *IEEE Access*, vol. 7, pp. 108304–108315, 2019.
[17] M. Li, R. Zheng, L. Liu, and P. Yang, "Extraction of threat actions from threat-related articles using multi-label machine learning classification method," in *Proc. 2nd Int. Conf. Saf. Produce Informatization (IICSPI)*, Chongqing, China, Nov. 2019, pp. 428–431, doi: 10.1109/IICSPI48186.2019.9095885.
[18] G. Xu, Y. Zhang, L. Jiao, E. Panaousis, K. Liang, H. Wang, and X. Li, "DT-CP: A double-TTPs-based contract-signing protocol with lower computational cost," *IEEE Access*, vol. 7, pp. 174740–174749, 2019.
[19] T. Kim and D. J. Allstot, "A tunable transmission line phase shifter (TTPS)," in *Proc. IEEE Int. Symp. Circuits Syst.*, vol. 1, May 2004, p. I-972.
[20] P. Kampanakis, H. Perros, and T. Beyene, "SDN-based solutions for moving target defense network protection," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2014, pp. 1–6.
[21] S. Debroy, P. Calyam, M. Nguyen, A. Stage, and V. Georgiev, "Frequency-minimal moving target defense using software-defined networking," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2016, pp. 1–6.
[22] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: Transparent moving target defense using software defined networking," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.* Aug. 2012, pp. 127–132.
[23] Z. Zhao, F. Liu, and D. Gong, "An SDN-based fingerprint hopping method to prevent fingerprinting attacks," *Secur. Commun. Netw.*, vol. 2017, Feb. 2017, Art. no. 1560594.
[24] A. Chowdhary, S. Pisharody, A. Alshamrani, and D. Huang, "Dynamic game based security framework in SDN-enabled cloud networking environments," in *Proc. ACM Int. Workshop Secur. Softw. Defined Netw. Netw. Function Virtualization*, Mar. 2017, pp. 53–58.
[25] J. Hong, "The state of phishing attacks," *Commun. ACM*, vol. 55, no. 1, pp. 74–81, Jan. 2012.
[26] M. Thompson, N. Evans, and V. Kisekka, "Multiple OS rotational environment an implemented moving target defense," in *Proc. 7th Int. Symp. Resilient Control Syst. (ISRCS)*, Aug. 2014, pp. 1–6.
[27] C. Lei, D.-H. Ma, and H.-Q. Zhang, "Optimal strategy selection for moving target defense based on Markov game," *IEEE Access*, vol. 5, pp. 156–169, 2017.
[28] S. Neti, A. Somayaji, and M. E. Locasto, "Software diversity: Security, entropy and game theory," 2017.
[29] I. E. Mir, A. Chowdhary, D. Huang, S. Pisharody, D. S. Kim, and A. Haqiq, "Software defined stochastic model for moving target defense," in *Proc. Int. Afro-Eur. Conf. Ind. Advancement*. Cham, Switzerland: Springer, 2016, pp. 188–197.
[30] A. Clark, K. Sun, L. Bushnell, and R. Poovendran, "A game-theoretic approach to IP address randomization in decoy-based cyber defense," in *Proc. Int. Afro-Eur. Conf. Ind. Advancement*. Cham, Switzerland: Springer, 2015, pp. 3–21.
[31] L. Bekdemir, "Hybrid probabilistic timing analysis with extreme value theory and copulas," Ph.D. dissertation, Middle East Tech. Univ., Ankara, Turkey, 2019.
[32] E. A. Sharma, *Computer Programming and IT*. New Delhi, India: Laxmi Publications, 2012.
[33] R. Patgiri, S. Nayak, and S. K. Borgohain, "Role of Bloom filter in big data research: A survey," 2019, *arXiv:1903.06565*. [Online]. Available: http://arxiv.org/abs/1903.06565
[34] M. B. Khan, "Advanced persistent threat: Detection and defence," 2020, *arXiv:2004.10690*. [Online]. Available: http://arxiv.org/abs/2004.10690
[35] Y. D. Lin, "Editorial: Second quarter 2020 IEEE communications surveys and tutorials," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 790–795, 2nd Quart., 2020.
[36] P. Bhatt, E. T. Yano, and P. Gustavsson, "Towards a framework to detect multi-stage advanced persistent threats attacks," in *Proc. IEEE 8th Int. Symp. Service Oriented Syst. Eng.*, Apr. 2014, pp. 390–395.
[37] Q. Su, Y. Tang, Z. Li, K. Liu, and T. Cheng, "Analysis of the structure of hive files and the implementation of pivotal operations for distributed computing environment," *Cluster Comput.*, vol. 22, no. 3, pp. 5675–5689, 2019.
[38] A. Flaih, C. Akmyradov, J. Guardiola, and H. Elsalloukh, "Statistical analysis of the BIESEP ROC curve," Tech. Rep.
[39] M. Revathi and T. Ramesh, "Network intrusion detection system using reduced dimensionality," *Indian J. Comput. Sci. Eng.*, vol. 2, no. 1, pp. 61–67, 2011.
[40] A. Moumena, "Quickest physical-layer MGD anomaly detection for jamming attacks in centralized modulated wideband converter-based ROC curve," *Int. J. Commun. Syst.*, vol. 32, no. 18, p. e4159, Dec. 2019.
[41] M. D. Hossain, H. Ochiai, F. Doudou, and Y. Kadobayashi, "SSH and FTP brute-force attacks detection in computer networks: LSTM and machine learning approaches," in *Proc. 5th Int. Conf. Comput. Commun. Syst. (ICCCS)*, May 2020, pp. 491–497.
[42] S. Zavrak and M. Iskefiyeli, "Anomaly-based intrusion detection from network flow features using variational autoencoder," *IEEE Access*, vol. 8, pp. 108346–108358, 2020.
[43] A. Sorokin, D. Galkin, E. Ivanayskiy, and A. Shubochkin, "Quantitative assessment of radiographic control informativeness using ROC analysis," *J. Phys., Conf. Ser.*, vol. 1327, no. 1, Oct. 2019, Art. no. 012013.
[44] X. Wang, Q. Liu, Z. Pan, and G. Pang, "APT attack detection algorithm based on spatio-temporal association analysis in industrial network," *J. Ambient Intell. Humanized Comput.*, 2020.
[45] P. Arnoth and M. Cserna, U.S. Patent 16 315 086, 2019.
[46] E. Marková, T. Bajtoš, P. Sokol, and T. Mézešová, "Classification of malicious emails," in *Proc. IEEE 15th Int. Sci. Conf. Inform.*, Nov. 2019, pp. 279–284
[47] G. Saad and M. A. Raggi, "Attribution is in the object: Using RTF object dimensions to track apt phishing weaponizers,"
[48] I. K. P. Stellios and M. Psarakis, "Advanced persistent threats and zero-day exploits in industrial Internet of Things." in *Security and Privacy Trends in the Industrial Internet of Things*. Cham, Switzerland: Springer, 2019, pp. 47–68.
[49] J. Gassen and J. P. Chapman, "HoneyAgent: Detecting malicious java applets by using dynamic analysis," in *Proc. 9th Int. Conf. Malicious Unwanted Softw., Amer. (MALWARE)*, Fajardo, Territory, Oct. 2014, pp. 109–117, doi: 10.1109/MALWARE.2014.6999402.
[50] A. Paradise, A. Shabtai, R. Puzis, A. Elyashar, Y. Elovici, M. Roshandel, and C. Peylo, "Creation and management of social network honeypots for detecting targeted cyber attacks," *IEEE Trans. Comput. Social Syst.*, vol. 4, no. 3, pp. 65–79, Sep. 2017.
[51] X. Han, T. Pasquier, A. Bates, J. Mickens, and M. Seltzer, "UNICORN: Runtime provenance-based detector for advanced persistent threats," 2020, *arXiv:2001.01525*. [Online]. Available: http://arxiv.org/abs/2001.01525
[52] A. S. M. M. Jameel, A. P. Mohamed, X. Zhang, and A. E. Gamal, "Deep learning for frame error prediction using a DARPA spectrum collaboration challenge (SC2) dataset," 2020, *arXiv:2005.01446*. [Online]. Available: http://arxiv.org/abs/2005.01446
[53] W. Wang, B. Tang, C. Zhu, B. Liu, A. Li, and Z. Ding, "Clustering using a similarity measure approach based on semantic analysis of adversary behaviors," in *Proc. IEEE 5th Int. Conf. Data Sci. Cyberspace (DSC)*, Jul. 2020, pp. 1–7.
[54] J. Singh, H. Ramchetty, and A. Gupta, U.S. Patent 10 148 693, 2018.
[55] B. Wang, Y. Yao, S. Shan, H. Li, B. Viswanath, H. Zheng, and B. Y. Zhao, "Neural cleanse: Identifying and mitigating backdoor attacks in neural networks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 707–723.

NACHAAT MOHAMED (Member, IEEE) is currently pursuing the Ph.D. degree in cyber-threat management (APT - ATT&CK) with the Universiti Sains Malaysia. He is an Associate Manager Emerging Technology Risk & Cyber with KPMG Malaysia. He is a member of ISACA. He is leading cyber defines team in KPMG to conduct VAPT inside/outside Malaysia. He is more than 17 years of successful experience in cyber security and IT risk management. He is an expert in cyber security management, threat intelligence, cyber defines, cyber response, protect governments/organizations against APT attacks, Annomali TIP, APT, MITRE, Red/Blu/Purple Teaming, OSINT, TTPs, IoC, ATT&CK, STIX, TAXII, PCI DSS, NIST 800-53, COBIT 5, CIS benchmark, ISO 27001, and SANS. He has achieved goals of organizations, building brands, building people, and strategist. He provided CDP workshops, cyber security awareness training, and reverse engineering sessions to several clients and universities in Malaysia. He worked seven years as an oracle developer and a database administrator, using Oracle 8i, 9i, 10g, 11g report/form 6i, IBM Cognos, and IBM DataStage. He is programming by SQL, PL/SQL, and Python. He has a high knowledge in blockchain, the IoT, ICS, HMI, PLC, SCADA, DCS, and RPA. He was able to publish seven articles in Scopus, and ISI journals. He is carried many professional certifications CISM | CRISC | CDPSE | ECSA | CTIA | CEH | CEH PRACTICAL | CHFI | CNSS | IBM-DS | OCA | OCS | MCCT | ATT&CK.

BAHARI BELATON received the bachelor's degree in computer science from the South Australian Institute of Technology, Australia, in 1989, and the Ph.D. degree from Leeds University, U.K., in 1995. He is currently the Dean of the School of Computer Sciences (SOCS), USM, Bahari, who belongs to the Semai tribe of Tangkai Cermin in Perak, also added another feather to his cap when he was appointed National Advanced IPv6 Centre (NAv6) director. With these two appointments, he is believed to be the first Orang Asli to be appointed as a dean in Malaysian history and also the first to hold two head of department positions simultaneously in an institution of higher learning in Malaysia. He was known for his expertise in areas of scientific data visualisation, computer graphics and network security, he has served with USM for more than 24 years and achieved numerous successes throughout his career, especially with regards to academic development and research. His aim in life is to serve, provide his expertise and contribute his capabilities to USM, his students, his community and his family. To fulfill a requirement by the Malaysian Public Service Department (JPA), which specifies that those who intend to serve in the public sector need to have an honors degree, he then pursued an additional year of study at Flinders University, Australia, in 1991, to obtain an honors before completing his Ph.D. degree.