

State-of-the-Art in Chinese APT Attack and Using Threat Intelligence for Detection. A Survey

Nachaat Mohamed¹

¹ *Rabdan Academy - Abu Dhabi, UAE. ORCID 0000-0002-4202-1294*

Email: ¹eng.cnel@gmail.com

Abstract

This survey is Chinese Advanced Persistent Threat (APT) real attack groups and scenarios. This survey provides a taxonomy of Chinese APT groups/attacks in conjunction with the use of Threat Intelligence (TI) to detect and prevent the attacks. This paper will provide the current knowledge and emerging APT groups that target governments and private enterprises. In addition, this paper presents, contributions, performance comparison and methods of criticism of detection in the current solutions. The study covers many attack groups funded by different Chinese governments to attack other governments around the world, taking into account that each group is specialized to attack specific sectors, some of them attack the military, police and intelligence departments, and some attack the banking, commercial and agricultural sectors, and some attack the information technology, health, arts, and nanotechnology sectors, etc. In this paper, we propose solutions at the first potential victim, and at the network, level to stop APT attacks. We recommend that there must be multi-layer protection over the first machine and infrastructure to detect and prevent APT attacks. This Paper will use adversarial tactics techniques and common knowledge (ATT&CK) as a knowledge base. We recommend researchers focus on ATT&CK, and TI to develop a solution against APT attacks.

Keywords: APT. Covid-19. Attack. Exploit. Threat Intelligence, Nation State.

I. INTRODUCTION

In the event there's one thing that keeps corporate cybersecurity experts alert at night, it's the thought of an assault utilizing an extent of advanced strategies planned to take the company's important information. advanced persistent threat (APT) uses nonstop, covert, and modern hacking strategies to pick up get to a framework and stay interior for a delayed period, with possibly damaging results. Since of the level of exertion required to carry out such an attack, APTs are more often than not levelled at tall esteem targets, such as nation states along with other enterprises. instead of basically plunging in and clearing out rapidly, as numerous dark cap programmers do amid lower-level cyber assaults. APT could be a strategy of assault that ought to be on the radar of businesses all over. Be that as it may, this doesn't cruel that little- and medium-sized

businesses can overlook this sort of attack. APT assailants are progressively utilizing littler companies that make up the supply chain of their extreme target as a way of picking up get to huge organizations. They utilize such companies, which are regularly less well-defended, as stepping-stones. Since corporate cyber protections tend to be more advanced than a private user the strategies of assault frequently require the dynamic inclusion of somebody on the interior to attain that pivotal, all-important crowbar minute. That doesn't be cruel, in any case, that the staff part intentionally takes part in the assault. It regularly includes an assailant conveying a run of social designing procedures, such as whaling or stick phishing. Advanced persistent threat (APT) may be an incognito cyber assault on a computer arrange where the assailant picks up and keeps up unauthorized get to the focus on

arranging and remains undetected for a critical period. able to say the various entities large and little, open division and private can advantage from an effective progressed tireless risk. Numerous suspects that governments and country states have utilized Well-suited assaults to disturb particular military or insights operations. Cases incorporate the Titan Rain, Ghostnet, Stuxnet assaults and others. In expansion, littler bunches are utilizing easier apparatuses, such as social building, to pick up get to and take mental property. and the foremost vital question is what is the way to detect and prevent APT attacks? This may be a stacked question, when organizations identify holes in their security, they instinctively convey a standalone item to fill that void. An arrangement filled with standalone items, be that as it may, will continue to have characteristic gaps. To maintain a strategic distance from these holes in security, organizations ought to take a holistic approach. This requires a multi-layered, coordinated security arrangement. Conveying a portfolio of items that can consistently work together is a perfect way the most perfect way to improve security.

II. MAIN TEXT (ATT&CK)

Model which is a knowledge base that businesses can employ to improve resistance, meanwhile giving the researchers ability to understand the behavior and real scenarios used by APT attacker groups. The ATT&CK is utilized as an establishment for the advancement of particular risk models and strategies within the government, and private sectors, Simultaneously, within the cybersecurity item and benefits community [5]. MITRE Shield is a dynamic defines information base MITRE is creating to capture and organize what is being learned around dynamic defines an enemy engagement [13]- [33]. Most security arrangements cover the MITRE ATT&CK strategies within the early or afterward parts of the assault cycle. Whereas the Attivo Systems Threat Defend solution gives scope over 11 of the 12 strategies in MITRE ATT&CK, it gives the foremost scope for those that happen post-

compromise – Credential Get to, Revelation, Sidelong Development, Collection [6]. These stages are where enemies spend most of their time after they avoid guards and burrow more profound into the organization, and where conventional security controls battle to distinguish their actions. With the Threat Defend stage, organizations gain visibility and discovery of these strategies early within the crime cycle. The behavioral matrix ATT&CK displayed by MITRE contains the taking after centre components:

Tactics: ATT&CK, or Adversary Tactics, Techniques, and Common Knowledge is a methodology for understanding the methods used by malicious actors in order to better protect your organization from cyber-attacks. MITRE Corporation is responsible for the development of the ATT&CK framework, which is now used by both the commercial and governmental sectors. The framework provides a common language for discussing cyber threats and can be used to develop defenses against specific tactics employed by bad actors [7].

Techniques: Identifying and preventing risks to a business is the primary objective of any information security programme. It is essential to maintain a well-rounded security posture that addresses all conceivable attack vectors in order to achieve this successfully [8]. There are several frameworks for recognising and mitigating risks, but one of the most thorough is MITRE's ATT&CK method matrix. This is a list of known malicious strategies and approaches. For everyone in the company, it serves as a common language. Fortification Meade Try (FMX) was developed in 2013 as a consequence of MITRE's analysts imitating both adversary and defender behaviour in an effort to go ahead post-compromise location of risks through telemetry detection and behavioural evaluation. How well are we doing at spotting archival adversary behaviour? That was the big question for the analysts. ATT&CK, an instrument for classifying enemy conduct, was devised by analysts to address this

topic [9]. Methods used by the enemy to attain their goal are included in the MITRE ATT&CK framework. Within the ATT&CK Lattice, these locations are classified as tactics. The objectives are laid out sequentially, from the point of observation to the final aim of exfiltration.. ATT&CK for Undertaking, which includes Windows, MacOS, Linux, AWS, GCP, Skyblue, Office 365, SaaS, and Arrange circumstances, categorises the taking after opponent methods:

Reconnaissance: In order to plan future activities, the opponent is gathering information. Reconnaissance is a strategy that focuses on acquiring information from the enemy that may be used to enhance targeting. It's possible that this data includes details on the casualty organisation, structure, or staff/staff members. The APT may make use of this data to aid in subsequent phases of the APT lifecycle, such as managing and completing Introductory Make sure you know where you want to go when the deal is done or lead and support other people in their efforts to do so [10].

Resource Development: The enemy is striving to amass resources that they can use to aid their own efforts. Enemies may improve their resources by manufacturing, acquiring, or compromising/stealing assets that can be used to support their emphasis on [11]. " Foundations, accounts, and capabilities all fall within this category. As part of the enemy's lifecycle, these assets may be used in different ways, such as bolstering Command and Control, obtaining mail accounts for phishing as part of initial access, or stealing code marking certificates to bypass defences [11].

Initial Access: Their network is under attack from the adversary. Initial One should use a variety of approaches to ensure that the beginning point of the arrangement is stable. The methods used to get a foothold include spear phishing and exploiting flaws in publicly accessible web servers. It's possible that the

toeholds gained in the first access may allow for further access, such as large accounts and the use of outside administrations, or even restricted usage owing to changing passwords [12].

Execution: Pernicious code is being attempted by the APT. Adversary-controlled code may execute on a local or distant framework using this strategy. All other measures, such as studying structured data, are often paired with methods that execute malicious code. An attacker may, for example, use an unreachable tool to execute a PowerShell script that discloses more frameworks. [13].

Persistence: The enemy/attacker is attempting to keep up a foothold working over the target infrastructure. this tactic (persistent) comprises strategies that foes utilize to keep getting to frameworks over restarts, changed accreditations, and other intrusions that might cut off their get to. Methods utilized for perseverance incorporate any get to, activity, or setup changes that let them keep up their conventional balance on systems, such as supplanting or highjacking the current applications [14].

Privilege Escalation: Higher-level permissions are being sought by the adversary. The term "Privilege Acceleration" refers to techniques used by adversaries to gain access to greater levels of agreement on a system or plan. An enemy may commonly enter and explore an agreement with the underprivileged, but they need to seek their permission before they can take action. Common methods include exploiting system flaws, misconfigurations, and vulnerabilities [13]. As OS highlights that allow an opponent to hang on may perform in a higher situation, these techniques typically cover using Tirelessness ways [15].

Defense Evasion: The adversary is striving to evade detection. Enemies use a variety of tactics in order to keep their location a secret during a compromise. Defending avoidance

methods include removing or deactivating security computer programmes or obfuscating or encrypting data and scripts.. It isn't only trustworthy forms that are used by the enemy to hide and conceal their virus. There is a cross-listing of methods for other approaches when the benefit of subverting guards is mentioned [14].

Credential Access: The foe is attempting to take account names and passwords. credential access tactic is comprised of methods for taking qualifications like account names and passwords. Strategies utilized to urge accreditations incorporate keylogging or credential dumping. Utilizing true blue accreditations can grant foes get to frameworks, make them harder to detect, and allow forming more accounts to assist accomplish their objectives [16] -[37].

Discovery: The APT is scouring your system for information about itself. In order for an adversary to get knowledge about a target's structure and internal organisation, he or she employs a variety of methods. Adversaries who are keeping a close eye on the environment and putting themselves in a position to make a decision may benefit from these tactics. They also allow adversaries to examine what they can control and the surrounding area to see whether it may help them achieve their present goal. This post-compromise information collection goal is often achieved via the use of local working framework devices [18]- [39].

Lateral Movement: Attempts are being made by the adversary to traverse your surroundings by you. The LM technique is a set of processes that adversaries use to gain access to and control over systems inside an organisation that are otherwise unavailable. There are times when the primary goal is to investigate the organisation in order to find their aim and therefore get there. Coming to their objective frequently includes rotating through different frameworks and accounts to pick up. Foes might introduce their remote get to apparatuses

to achieve Sidelong Development or utilize authentic accreditations with local arrangements and working framework devices [2]- [39].

Collection: This means the foe/adversary is attempting to assemble information of intrigued to their goal. The data collected by APT groups comprises procedures foes may utilize to assemble data and the sources information is obtained from target environments. After gathering information, the next step is to take (exfiltrate) the data. Different drive types, browsers, music, video, and email are all common target sources. Screenshots and console input are two of the most common ways to gather data. [33].

Command and Control: Compromise frameworks are being targeted by the opponent, who is trying to connect with them. As part of a casualty network, an enemy's command and control processes may be used to connect with frameworks under their control. It is usual for adversaries to mimic ordinary, expected behaviours in order to maintain a strategic distance from the target. Depending on the victim's established structure and resistances, a foe/adversary may set up command and control in various degrees of stealth [37].

Exfiltration: The enemy is trying to steal information. Enemies' strategies for stealing information from your company are included in the exfiltration strategy. In order to avoid notice while expelling the information they've gathered; foes often bundle the information they've obtained. Encryption and compression will be moved to a new location, most likely in a different nation. Getting information out of a target group often involves exchanging it across their command-and-control channel or a replacement channel, and may also include setting a restriction on the transmission of the information.

Impact: The frameworks and data are under attack from the enemy/adversary. Trade and operational forms may be used by foes to

disrupt access or corrupt judgement, causing a ripple effect. Crushing or modifying data might be one of the procedures used to have a desired impact on target organisations. In certain circumstances, trade forms may seem to be good, but they may have been altered to benefit

the opponents' objectives. They might be exploited by enemies to carry out their end goal using these tactics employed in the impact strategy [13].

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Escape to Host	Direct Volume Access
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)
Search Victim-Owned Websites			System Services (2)	User Execution (3)	Hijack Execution Flow (11)	Exploitation for Defense Evasion
			Windows Management Instrumentation	External Remote Services	Process Injection (11)	File and Directory Permissions Modification (2)
				Hijack Execution Flow (11)	Scheduled Task/Job (6)	Hide Artifacts (9)
				Implant Internal Image	Valid Accounts (4)	Hijack Execution Flow (11)
				Modify Authentication Process (4)		Impair Defenses (9)
				Office Application Startup (6)		Indicator Removal on Host (6)
				Pre-OS Boot (5)		Indirect Command Execution
						Masquerading (7)
						Modify Authentication Process (4)
						Modify Cloud Compute Infrastructure (4)

FIGURE 1. ATT&CK from reconnaissance tactic to defences evasion tactic

Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 11 techniques
Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Modify Authentication Process (4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
OS Credential Dumping (8)	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
Steal or Forge Kerberos Tickets (4)	Network Service Scanning		Data from Removable Media	Protocol Tunneling		Service Stop
Steal Web Session Cookie	Network Share Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
Two-Factor Authentication Interception	Network Sniffing		Email Collection (3)	Remote Access Software		
Unsecured Credentials (7)	Password Policy Discovery		Input Capture (4)	Traffic Signaling (1)		
	Peripheral Device Discovery		Screen Capture	Web Service (3)		
	Permission Groups Discovery (3)					
	Process Discovery					
	Query Registry					

FIGURE 2. ATT&CK from credential access tactic to impact tactic.

III. APT GROUPS

common title within the security community. Examiners track clusters of exercises utilizing different explanatory techniques and terms such as danger bunches, movement bunches, danger performing artists, interruption sets, and campaigns. A few bunches have numerous names related to comparable exercises due to different organizations following comparable exercises by diverse names. There may be some overlap between the definitions acquired by different organisations and the definitions gathered by the same organisation [19]. The MITRE ATT&CK team uses the word "Gather"

to refer to any of the extra assignments for a cluster of hostile activity on the "Gather" pages. Tracking coverings between names based on fully specified connections, which are allocated as linked organisations is the primary goal of the group's efforts. We do not refer to these names as proper covers, and we encourage examiners to do more research on their own. " Maps of the techniques used by each group are provided, as well as a list of unique identifiers. Data provided does not include all Bunch methods, but just those that can be accessed via open-source documentation [20].

1- ADMIN@338: is a Chinese cyber-attack group. The ADMIN@338 attacker group is a well-known hacking collective that has been operating since at least 2014. The group is known for its widespread attacks against both governments and private businesses, and it is believed to have links to the Russian government. In early 2017, the group was involved in a high-profile attack against the Ukrainian power grid that left tens of thousands of people without power. Admin@338 used Applications such as BUBBLEWRAP, ipconfig, LOWBALL, Net, netstat, PoisonIvy, Systeminfo. And regarding the techniques used by admin@338 are Account Discovery [22].

2- APT41: Most of APT41's covers, including BARIUM and Winnti Gather, include open detailing at the very least. Within APT41's synchronised activities, the group's state-sponsored action and claim cybercrime operations can be seen [21]. APT41 has consistently operated its claim-financially-motivated efforts alongside surveillance operations throughout its career [21]. On the other hand, APT41's covert operations have altered fundamentally over time, implying adjustments in assigned missions or current contracts to the total. While APT41 has shifted its focus from stealing mental property to obtaining vital insights and setting up access points, FireEye believes this is consistent with other Chinese surveillance administrations. Whatever the case may be, the group's continued interest in the video game business for financial reasons has been unaffected. – It has been almost two years since we last saw evidence of IP theft. – As recently as 2014, APT41 was seen conducting surveillance efforts in tandem with economically motivated disruptions, demonstrating their ability to change several objectives at the same time. While the group was still running financial-motivated efforts, including long-term disruptions, which often lasted more than six months, surveillance operations took place. While the group was still conducting financially persuaded efforts, including longer-term pauses

that normally escalated for more than a year [24], secret events processes emerged. By infecting legitimate server software packages used by hundreds of companies around the world every year since 2017, APT41 exercises have included an arrangement of supply chain compromises, limiting the deployment of additional payloads to selected targets while injecting malware into those legitimate packages. To support a large organisation, APT41 specialised in medical devices from July 2014 to May 2016 [25]. 30 percent of the victims of APT41 were linked to a backup firm specialising in the fabrication of medical and other infrastructure equipment. In the operation, the use of spoofed/hacked domains and watchword strings indicates a contract tasking to attack a backup rather than the parent company. Based on the characteristics of the targeted hosts, we may infer that APT41 was particularly interested in medical device backup personnel and programmes. GEARSHIFT, a key logger, was to be given to the firm that makes healing gadgets. One of the victim's advanced certificates was hacked and used to sign malware that was used to attack a lone biotech business, as will be discussed in more detail below. Earlier this year, APT41 had its sights set on a biotech firm with a history of security issues. Deeply sensitive information about practically all of the company's activities, including its human resources, was targeted. Clinical trials data, academic data, and R&D funding-related papers were stolen. These two campaigns were most likely carried out simultaneously, as shown by the time drawing, use of the same GEARSHIFT sample, and an advanced certificate from the aforementioned medical device manufacturer. Fireeye's 2018 report said that APT41 was targeting healthcare sectors, despite the fact that their goals throughout this compromise/organization were unclear. Hundreds of firms throughout the globe employ the malware-infected server software, but the operation restricts the distribution of further payloads to a few selected targets [26]. Among the many methods APT41 use to infiltrate its targets, including

DNS, Web Protocols, and File Transfer Protocols, are some that are classified as Application Layer Protocols. By making use of the data's usefulness, archive it at BITS Start up or sign in The Registrar's Office Execution Has Begun Automatically Start-up directories / key shortcuts attacks on passwords or brute force Using the Windows Key Unix's shell command interpreter PowerShell is the shell's scripting and command interpreter. A New User Account Is Created: Invent or re-work This is a Windows-based programme. A local system's data is encrypted and used for Impact. Algorithms for Domain Generation and the Execution of Dynamic Resolution Triggered by an Event: Implementation barriers include Disabled External Services (DES), Fallback Channels (FC), File and Directory Detection (DDD), and the Environment Keying (EKE). These techniques are all instances of hijacking the execution flow: DLL search order hijacking, DLL side loading and dynamic linker hijacking Deleting Windows event logs, command history, files, and the Ingress Tool are all part of the process of removing indications from the host machine. Keystroke Recording By modifying the register, for example, a job or service might be disguised as another task or service, for example. Using a tool, you may learn new skills. Leakage of OS Passwords: Pre-OS boot options include LSASS Memory Spear phishing Attachment, Phishing Process Injection, and Proxy. Protocol for Remote Desktop Access, or RDP Admin Shares, SMB Hijacking, Rootkits, and Windows Hijacking: Making a Timetable for a Project Job Execution Scheduling Privileged Binary Proxy Methods Other Trust Controls include code signing for the compiled HTML file and Rundll32 executable. Other system services and constraints on the software supply chain, detection of the system network configurations and networks of system connections and identification of the system owner and user These two web services are Windows Management Instrumentation (WMI) and Dead Drop Resolver (DDR). BITSAdmin, Certutil, China Chopper, Cobalt Strike, Derusbi, Empire

FTP gh0st RAT, ipconfig and MESSAGETAP were all utilised by APT41. njRAT and PlugX PowerSploit were also used. [13]- [39]- [33]- [2]- [20].

3- **APT30:** There is little to no need for China's APT organisation, which has the power to compromise organisations across the area and subcontinent if it is left uncontrolled. APT30 prioritises its targets, collaborates in shifts and builds malware according to a sequential progression plan, according to our malware research. Their missions, which concentrate on obtaining sensitive information, include a wide range of targets, including secret government systems and networks that aren't accessible through a typical Web connection. Since 2005, even though they were not initially designed to attack networks with air gaps, the APT30 team seems to have kept this in mind throughout their development efforts. To demonstrate their long-term ambitions, APT30 has been working on a set of coordinate tools over the last decade and has reused the foundation. Backdoors and downloaders may be used to infect portable CDs and infiltrate air-gapped networks in order to steal data from them. APT30 often sets up its own DNS names in order to disseminate malware (C2). As can be observed by the frequency with which they emerge in malware testing, several of these areas have been in use for quite some time. APT30's malware exhibits an organised and well-ordered approach that is typical of a cooperative team environment. They and the engineers that assist them mark and monitor their viral versions in a meticulous manner in order to keep tabs on their infection. Mutexes and occasions are used to ensure that the malware version data is contained in the binary to ensure that only one copy of the infection is running at any one time. Any time Malware C2 sends a message to the malware, it immediately checks for newer versions of itself. Lecna backdoor controller software from APT30 indicates that threat actors prioritise their targets and work in shifts. To determine whether or not the victim should connect with the attackers' primary controller, the APT30

backdoors often employ a two-stage C2 handle. The controller's graphical user interface allows operators to prioritise hosts, write comments to victims, and set alerts for specific hosts that appear (GUI). Unused speech boxes have finally appeared after months in the current attack's control panel [29]. The APT30 virus may also infect portable discs that have the potential to hop over network gaps and steal data in rare cases (such as certain record kinds). Malware that can be "hidden" and stay undiscovered on a victim's computer for a lengthy period of time, presumably for long-term persistence, may be written. For the most part, it is a major APT group that is focused on governmental intelligence targets. Southeast Asia is by far the most prevalent region for APT30's victims. Many signs indicate that the organisation has an interest in China's territorial politics and the legitimacy of the country's leadership in addition to disputed territory. Eventually, groups like APT39, which sign up for remote access in order to acquire information for criminal reasons, will stop using them. After being in use for almost five years in certain cases, the APT30 domains from the beginning are still being used as of late 2014 [30]. FireEye identified the md5 hash b2138a57f723326eda5d2dec56851 as one of the most punctual BACKSPACE viruses it has ever seen on March 11, 2005 at 00:44:47. The key C2 area in the test was www.km-nyc.com. According to a Delete test on November 5, 2014, at 05:57:26, the domain was still being utilised as an additional C2 space. APT30 has used a surprisingly small amount of tools and backdoors since its start. Since their current

approach has been so effective, it's probable that they don't feel the need to enhance or expand on their arsenal. However, even though APT30 has used numerous auxiliary and supporting devices in the past, their primary tools, such as the Delete and NETEAGLE backdoors and a set of devices (SHIPSHAPE and SPACESHIP) accepted to be designed for contaminating (and stealing information from) air-gapped networks, have proven to be extremely reliable over time. As a result, APT30 may be able to modify and adapt its source code to meet the needs of their current targets (governments and commercial entities) [31]. Backdoor Delete has existed since at least 2005, and it is still being used today. The BACKSPACE system seems to be flexible and modular, enabling it to adapt to changing needs over time. More information may be gleaned about APT30 by examining its BACKSPACE backdoors using the GUI controller used to monitor the group's activities. Third-party security firm FireEye utilised one sample of the Net Eagle Farther Control System (NEFCS) to test and assess three copies of the malware. Although the APT30 controller computer programme was written separately in 2010, 2011, and 2013, FireEye's portrayal of the tool's depiction demonstrates that the tool's depictions reflect its distinctiveness. The Delete controller may be equipped with a high-end GUI device. The "Menu" part of the controller's home screen also includes "About" information. The controller's hostname, internal and external IP addresses, framework uptime, and OS version and dialect are all shown on the bottom sheets [32].

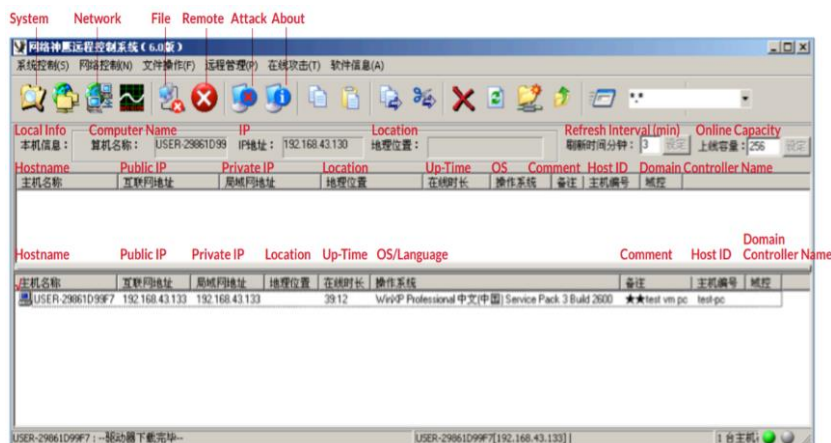


FIGURE 3. *APT 30 interface to control Long-Running Cyber Espionage Operation.*

APT30 using techniques such as Phishing: Spearphishing Attachment, User Execution: Malicious File, and malware such as BACKSPACE, FLASHFLOOD, NETEAGLE, SHIPSHAPE, and SPACESHIP [33].

4- APT3: Hackers from the Chinese APT organisation have the potential to carry out a continuous hacking campaign throughout the whole area and subcontinent without having to fundamentally modify their methods of operations. Using the evidence we've gathered from our malware research, we've deduced that the APT30 group prioritises its targets, works shifts in an open environment, and builds malware in a systematic manner. For the most part, their purpose is to obtain sensitive information from a broad variety of targets, including government systems that are not accessible to the general public. APT30 may not have started working on air-gapped networks with this goal in mind when they began their research and development in 2005, but it seems that they have had it in mind ever since. Over the last ten years, APT30 has worked on and enhanced a set of fundamental tools and reused the foundation. This speaks eloquently about their long-term aspirations. In order to infect detachable devices, cross air-gapped networks, and steal data, all the necessary tools are contained in the suite of software. APT30 often sets up its own DNS domains for command and control purposes (C2). During virus testing, several of the slots seem to have been in use for some time. Malware from APT30, for example, is organised and well-structured to demonstrate a collaborative team environment, and its process is well documented. Malware versioning is a critical aspect of any organization's operations. [28] There is only one instance of the malware running at any one time thanks to mutex and occasion, and the malware version data is housed inside this programme. If the malware's C2 communications include a version check, it can keep itself up-to-date with the most recent release by updating itself on its own. Threat

actors are advised to prioritise their targets and work in shifts via APT30's BACKSPACE backdoor controller software, codenamed "Lecna." An attacker's primary controller can only be accessed by first connecting to a beginning C2 server. APT30 backdoors are used to achieve this on a regular basis. With the controller's built-in GUI, users may prioritise hosts, leave notes for victims, and set alerts for selected hosts when they come online. After months of difficulty, the control panel for the current attack [29] now shows unused conversation boxes. Portable CDs with the capacity to jump over conversation gaps may be infected with APT30 malware to steal data (such as specific record types). The "hidden" mode of certain malware allows it to stay unnoticed on the target machine for extended periods of time. Most of this critical APT group's efforts are focused on targets that might be beneficial to intelligence agencies. In Southeast Asia, the majority of APT30's victims have been slain. The organisation seems to be mainly concerned with territorial political and military problems, disputed regions, and the legitimacy of the Chinese government in its social engineering initiatives. As a threat, APT39 enlists space for damaging purposes and then abandons it. It's been more than five years since APT30's domain names were first registered, with some of its early spaces still in use as recently as late 2014. There is a BACKSPACE virus with an MD5 hash of 22138a57f723326ed8eda5a that FireEye has been investigating. On March 11, 2005, at 00:44:47, I constructed 26d2dec56851. For the C2 section of the test, we utilised www.km-nyc.com, which is a frequently visited website. That domain was still being used in a Delete test on November 5, 2014, 05:57:26 md5 hash 38a61bbc26af6492fc1957ac9b05e43. APT30 seems to have a surprising lack of tools and backdoors, despite its long history of activity. In the absence of development in extending or adding to the arsenal, it may be because they've been effective with their current strategy. It's widely agreed, however, that APT30's principal

attack tools have been the backdoors NETEAGLE and Delete, as well as the SHIPSHAPE, SPACESHIP, and FLASHFLOOD device set, all of which are capable of infecting (and stealing data from) air-gapped networks. APT30 has long relied on Delete and NETEAGLE. It seems that APT30 has made a conscious decision to contribute to the long-term growth and progress of what appears to be a specific set of devices, rather than simply exchanging one backdoor for another when more modern, adaptive, or feature-rich devices become available. When the APT30 (or the engineers who provide them with devices) or their victims (governments/private entities) have specific requirements, they may alter the source code to meet those requirements [31]. In use since at least 2005, the Delete backdoor has gone through various revisions. Thus, BACKSPACE seems to have a wide range of adaptability and modularity. Examining APT30 BACKSPACE backdoors' GUI controller will provide further information on almost all of their activities. FireEye investigated and evaluated a single sample of the Delete controller software, known as the NetEagle Farther Control System, which had three copies of it inspected and studied. Despite the fact that its compilations were generated in the 2010s, 2011s, and 2013, the FireEye tool's portrayals of APT30's unique controller computer programme are not a coincidence. In theory, the Delete controller might be equipped with a full-featured GUI. Additional menu choices may be found in addition to "About," including System, Network, File, and Remote controls. In the bottom sheets, the hostname, IP address, framework uptime, and OS version and dialect of the controller's victims are shown [32]. [13]-[33]-[39].

5- APT1: APT1 attacker group targeting Data Innovation, Aviation, Open Organization, Satellites and Broadcast communications, logical investigation and counseling, vitality, transportation, development and Fabricating, designing administrations, high-tech hardware, universal organizations, legitimate

administrations Media, promoting and amusement, route, chemicals, budgetary administrations, nourishment and farming, Healthcare, mining, and education are all related fields. More than 140 companies have been targeted by APT1 and it has shown the capacity and expectation to steal from many organisations at the same time. In English-speaking countries, the group focuses on organisations that compromise a broad range of enterprises. There are at least a few, if not hundreds, of human administrators in APT1's structure, based on its measurement. APT1Backdoor's trojan. It was a Trojan horse called Barkiofork. Backdoor, Ecltysm. Talbot,Backdoor. Trojan's Wakeminap is a great way to start the day. Trojan has a terrible name. Moody, Intimate. In the back entrance of Wales, Revard In order from [2] to [20] to [21].. Skewer phishing is the most often seen method of introducing a compromise. Slandorous links or hyperlinks may be found in the phishing emails that use this technique. To the recipient, the subject line and substance of the e-mail are usually important. In addition, APT1 creates webmail accounts using the identities of real persons. The vast majority of the time, APT1 gate crashers use backdoors that seem to be their own, such as Harm Ivy and Gh0st Rodent, which are openly accessible. More frequently than not over their tenure in the company, APT1 would bring contemporary backdoors since they claim more frameworks. Even if one of their backdoors ends up being discovered and removed, they still have other backdoors to fall back on. Over the course of many weeks, we are able to identify several APT1 backdoor families that have been dispersed across a victim organisation. Among the several methods used by APT1 is Account Discovery: a local account. Acquire a Domain Name System (DNS) Data Archive: Windows Command Shell, Automated Collection, and Command and Scripting Interpreter Domains, data from the Local System, and other infrastructure are compromised. There are two methods of collecting emails: one is local, the other is remote. Email Accounts, etc., must be set up.

Using a false name or location to deceive: Discovery of Shared Resources on the Internet Capabilities Acquired Through the Use of Acquire talents by using a tool Dumping of OS Credentials: LSASS Memory Spear phishing Attachment, Phishing It's called "spear phishing [13]- [33]- [39].

6- APT12: is a government-funded outfit that engages in hostile activities. Divisions to focus on: Government, defences, and writers overview: APT12 is widely believed to be a cyber-surveillance group affiliated with the People's Liberation Army of China. Targets set by the People's Republic of China (PRC) remain consistent with APT12's goals. This group's actions are in accordance with the PRC's goals and interests in Taiwan. Assault vectors: Mandiant watched APT12 convey these abuse records through phishing emails from substantial but compromised accounts, we anticipate the risk gathered to proceed to utilize phishing as a malware conveyance strategy [40]. APT 12 uses critical malware such as HIGHTIDE, RIPTIDE, WATERSPOUT, and THREBYTE. Meanwhile employ these techniques (Dynamic Resolution: DNS Calculation, Exploitation for Client Execution, Phishing: Spear phishing Attachment, User Execution: Malicious File, and Web Service: Bidirectional Communication) to accomplish the attacks.

7- APT16: China is said to be the source, Japanese and Taiwanese organisations in the high-tech, government administrations, media, and budgetary administrations sectors are the primary target groups. A group of people in China who are interested in Taiwan politics and journalism. Spear phishing emails delivered to Taiwanese media outlets and webmail addresses are the attack vectors used. A Taiwanese sell-off site requested information from draw reports for recruitment and subsequent posting of merchandise. [41].

8- APT17: is supported by the Chania government and is known as the Tailgator

Group, Delegate Dog (in Greek). China is said to be the source. Markets targeted include the federal government, as well as international legal firms and data-driven startups. Overview: Conducts organised disruption against companies that are the target of the disruption. Attack vectors, risk group used the ability to build profiles and post in groups to inject encoded CnC for use with a variant of the malware it employed. In addition, there are two advanced methods. Establish Accounts and Web Services Infrastructure. The CnC structure may remain dynamic for a longer amount of time if this approach makes it difficult for organised security specialists to determine the true location of the CnC. APT17 planned disruptions against the US government, the military sector, legal firms, data innovation businesses, mining industries, and non-governmental organisations (NGOs) in the US. [41].

9- APT19: It is a Chinese-based firm that has targeted a wide range of industries, from defences to money to vitality to pharmaceuticals to broadcast communications to high-tech education to manufacturing. Several legal and venture companies were targeted by a phishing attack in 2017. A few researchers believe that APT19 and *Profound Panda* are part of the same group, however open-source data does not support this. These are the groups we're trying to reach This organisation is presumably made up of legal and financial advisers, with some degree of Chinese government involvement. the *COBALTSTRIKE* trojan has been linked to *Signal*. Methods of attack: APT19 used a variety of techniques throughout 2017 to try to infiltrate targets. CVE 2017-0199, a vulnerability in Microsoft's Windows operating system, was exploited in early May by phishers. APT19 switched to using macro-enabled Microsoft Excel spreadsheets (XLSM) archives during the end of May. On the other hand, with regards to the APT's methodologies [40-42]. APT19 employs a wide range of attack methods, including Application-Layer Protocol

(ALP) attacks. Protocols for the Internet Login or Boot The Registry: Autostart Execution command line interpreter and scripting interpreter (such as PowerShell) Invent or Rework This is a Windows service. Encoding: Decoding, Deobfuscation, and Drive-by Compromise are all examples of data encoding. Disguised Window, Disguised Artifact, DLL Side-Loading, Registry Modification, Obfuscated Files or Information, and other methods of hijacking execution flow It's time to learn new skills. The Spearphishing Attachment, a phishing tool Registry Execution: Regsvr32, Rundll32, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery and User Execution: Malicious File [43].

10- APT28: The Common Staff Fundamental Insights Directorate, military unit 26165 in Russia, is said to be behind one of the world's most deadly APT organisations. Since at least 2004, this group has been dynamic [44]. the countries and military of eastern Europe, the NATO alliance as well as other European institutions of defence, are all part of the company's primary market niches. APT28 is a professional team of designers and administrators who are gathering important information on military and geopolitical concerns. In accordance with the time zones of Russia's main cities, including Moscow and St. Petersburg, this well-suited group runs malware testing using Russian dialect settings throughout business hours (8 a.m. to 6 p.m.). [44] This suggests that a well-established organisation, most likely the Russian government, provides APT28 with a steady supply of money and other resources. Exploitation for Privilege Escalation and Account Manipulation: Exchange Email Delegate Permissions are just two of the many methods APT28 use to infiltrate targets all over the globe. Acquire a Domain Name System (DNS) Vulnerability Scanning is an example of active scanning. There are two types of application layer protocols: the web protocols and the mail protocols. Archive the data you've

collected using a utility. Collection via Automated Means Invoke the Registry Run Keys / Startup Folder at boot or logon Logon or boot up Initialization Microsoft Windows Logon Script, Brute Force Squirting out your passwords PowerShell is a command and scripting language interpreter. Software that interprets and executes commands and scripts Transfer of Information Using Disposable Media, Data from repositories, SharePoint, local systems, network shared drives, and removable media Junk Data: Data Obfuscation, Staging of Data on-Site: Data Transfer Size Limits, Remote Data Staging, and more Reverse Encryption/Decryption of Files or Data Telephonic email storage and retrieval File and Directory Discovery, and Exploitation of Asymmetric Encrypted Non-C2 Protocol. Identify the Victim: Obtain Identity Credentials, Hidden files and directories may be used to conceal evidence. Disguised Window, Disguised Artifact, Delete Windows Event Logs to Remove Host Indicator Remove Host Indicator: File Deletion, Remove Host Indicator: Timestamp, Transfer Ingress Tool, Data Capture: Logging of keystrokes Network Denial of Service, Network Sniffer and Obfuscated Files or Information are all examples of inter-process communication. Acquire talents by using a tool NTDS, Peripheral Device Discovery, and LSASS Memory Dumping are all included in the Office Application Startup. There are several different types of Phishing: Spearphishing, Phishing for Personal Information, and more. Before OS Boot: Bootkit, Process Detection, etc. A third-party intermediary Proxy: Proxy with several hops, Rootkit, Screen Capture, Replication Through Removable Media, and SMB/Windows Admin Shares are some of the remote services available. Web Shell is a component of the server software. Execution of Signed Binary Proxy: Rundll32, Use Template Injection and Trusted Relationships to steal Application Access Tokens A Token, Pass the Hash, or an Access Token may be used as other authentication material. Malicious Link: User Execution, Malicious files, legitimate accounts,

and cloud accounts may all be executed by the user. Web service: two-way communication using a web browser.

11- APT29: APT29 is a hazardous group that Russia's Outside Insights Benefit is credited with creating (SVR). As of 2008, they have been working on government systems throughout Europe and NATO member states, conducting investigations and consulting with think tanks on a regular basis. The Law-based National Committee was reportedly hacked by APT29 in the summer of 2015 [45]. The SolarWinds supply chain breach cyber operation was attributed by the US and UK governments in April 2021 to the SVR open explanations, which included referrals to APT29. There were a slew of groups in North America, Europe, Asia and the Middle East that were wiped out by this effort. This campaign's on-screen characters were referred to as UNC2452, NOBELIUM, Stellar Particle, and Dim Corona by industry details. We know that APT29 has been gathering intelligence for the Russian Alliance since at least 2008 to support distant and security approach decision-making, according to an F-Secure analysis published in 2015: 'The Dukes are a well-resourced, exceptionally dedicated and structured cyberespionage group.' Both their ability to compromise their aims and their ability to operate with the exemption seem to be exaggerated among the Dukes. For the Dukes, Western governments and organisations including government services and offices, political think tanks and departmental outsourcers are the primary targets. Targets of theirs have also included Asian, African, and Central Eastern countries; groups linked to Chechen militancy; and Russian speakers who are involved in illegal drug and controlled substance exchanges. One of the most well-known APT29 malware toolsets is the CosmicDuke, a collection of malware that can be used to infect a wide range of systems. Dukes have engaged in large-scale stick-phishing efforts targeting hundreds or maybe thousands of legislative teachers in the last

several decades. Crush-and-snatch campaigns use a fast but noisy breaking followed by the rapid capture and exfiltration of as much information as possible [2]. [2] [2] As soon as the Dukes learn that the compromised target has value, they will turn to stealthier tactics that focus on continual compromise and extended compromise. In the West, Central Asia, East Africa, and the Middle East, this perilous on-screen figure targets government agencies and think tanks, as well as extreme Chechen groups. Unclassified systems in the White House, Department of Defense, and Pentagon were exposed in 2015 in a way that raised questions about their security. Onion, Sea, CloudDuke (also known as MiniDionis), and HammerDuke are all part of the APT29's collection of Duke-specific tools (aka Hammertoes). Nobelium, a Russian state-sponsored hacking group, has targeted more than 140 IT and cloud service providers, effectively penetrating 14 additional firms, Microsoft revealed on 25/10/2021. These attacks were part of an organised operation that began in May of this year, according to MSTIC, the Microsoft Risk Insights Center (MSTIC). Spear-phishing and password-spraying tactics targeted IT and cloud foundations departments, who are responsible for the security of their customers [44].

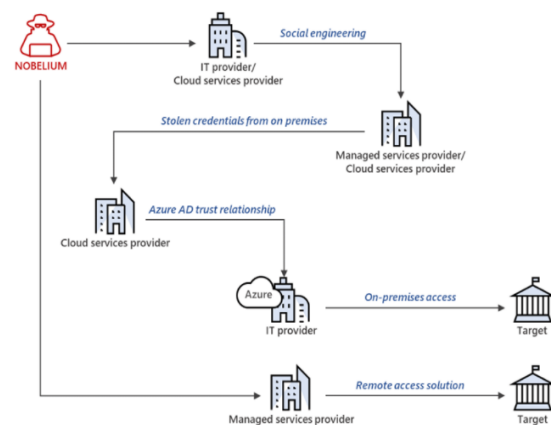


FIGURE 4. Example intrusion conducted by NOBELIUM demonstrating nested access across variety of methods. Source: Microsoft.com.

MSTIC has also identified nation-state activity related to the risk on-screen character NOBELIUM, who is attempting to gain access

to downstream clients of various cloud benefit suppliers (CSP), overseen benefit suppliers (MSP), and other IT administrations organisations (referred to as "service providers" for the rest of this web journal). These organisations have been granted regulatory or favoured access by other organisations, in addition to other service providers. Since May 2021, organisations with their headquarters in the Joined Together States and everywhere else in Europe have been under constant surveillance for any sign of movement. According to the results of MSTIC, NOBELIUM has initiated a campaign against these groups in order to leverage existing specialised belief links between supplier organisations and the government think tanks, as well as other corporations that these organisations support. This group and the one that attacked SolarWinds in 2020 have a number of parallels, and the actor's tactic of compromising one in order to compromise many was shown in the most recent effort. Microsoft has gotten in touch with known victims through our national notice handle and collaborated with both those victims and other industry partners to advance our investigation. This has led to the discovery of new information as well as the disruption of the harmful performer throughout this campaign. This is something that Microsoft has observed. Not only does NOBELIUM use a diverse and active arsenal of techniques to gain access to customer accounts, such as malware, watchword splashing, supply chain attacks, token theft, API manhandling, and spear phishing, but it is also possible that this strategy is a continuation of what they have been doing. Chairmen are required to implement stringent account security practises and take further efforts to safeguard their financial interests in order to prevent a recurrence of the assaults that were previously described. As part of the carefully monitored supply chain assaults, NOBELIUM also has its eyes set on the downstream customers and other businesses that benefit suppliers. As a consequence of these connections between providers,

consumers provide the supplier the power to manage the customers' inhabitants in the event that the supply was the chairman of the customer. This is a countermeasure that Microsoft has implemented. MSTIC is continuing to monitor, filter, and educate impacted customers and partners via our nation-state notification handle. Team Responsible for Location and Reaction at Microsoft In the meanwhile, Microsoft Danger Specialists have been working directly with customers who were affected by the event in order to help those clients in responding to the problem and managing the campaign's outstanding placement and direction. The misuse of underhanded ways and believe connections to target and pick up get to victims of intrigued for insights pick up has been a basic component of NOBELIUM's continuous progress over the last year. This has been the case particularly over the past year. Since that time, this has been shown by using the belief chain of benefits providers to get access to a diverse variety of client demographics for the sake of future assaults [33]. Instead of monitoring a big number of residents, NOBELIUM uses the standard trade hones that it has established to target downstream clients. The population that is being observed is very small. After their use has come to an end, these appointed authoritative benefits are no longer dynamic since they are neither evaluated for authorised use nor crippled by a benefit source or downstream client. Rather, after their usage has come to an end, they are no longer in use. The capacity of Nobelium to continue their efforts is rewarded if they have compromised the accounts that are related to their authorised regulatory advantages through earlier credential-stealing attempts. These accounts may be hacked to get access to Nobelium's regulatory advantages. According to the findings of a study conducted by Microsoft, businesses such as cloud service providers and other innovation organisations that oversee administrations for downstream clients are interested in and at risk of focusing on diligent risk performers. Furthermore, these businesses

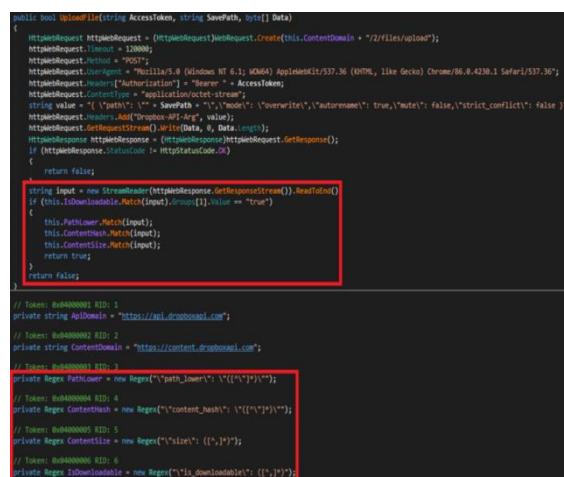
are at risk of doing so utilising a variety of strategies, ranging from credential get to focused on social building through genuine commerce forms and approaches. The mitigations and suggestions that are presented below offer additional information that may be used to determine how to find and prioritise appointed regulatory benefits. Vulnerability Active scanning may be shown through the process of scanning. The protocols that make up the Web are considered Application Layer Protocols. Archive the information making use of the benefits it offers. Log on or start the engine. Registry Run Keys / Startup Folder, There are a few different ways to automate the starting process, such using Boot or Logon. Steganography is a sort of data obfuscation that may be used to deobfuscate files or information or stage data in a place that is hidden from view. Develop Capabilities to Cause Malware: Building Capabilities: Electronic Signatures and Certificates Domain Policy Adjustments, Trust Discovery, and Trust Modifications, and Trust Modifications Infinite Resolving Power Message storage and retrieval through telephonic means The Windows Management Instrumentation, or WMI, consists of the following: Event-driven execution It is possible to generate web credentials such as Asymmetric Encrypted Non-C2 Protocol Exfiltration, You may reduce the effectiveness of your defences by turning off or modifying some tools, turning off Windows event logging, and modifying the system firewall. In addition, you have the ability to erase indications on the host, as well as files that have been deleted and timestomped, ingress tool transfers, masquerade, and information that has been obfuscated. Binary Filler, Software Packing, and Containerization Utilizing a tool will allow you to acquire skills. OS Credentials that are being dumped include DCSync, The Uncovering of Authorization Groups, Attachment: Phishing Link (also known as a Spearphishing Link), and Phishing: Attachment Fraud: The Practice of Phishing Using a Service: Spearphishing The uncovering of the procedure Domain Fronting Proxy, Internal

Proxy Proxy, and Multi-hop Proxy are all types of Proxies. For instance, you may make changes to your Windows system from a distant location by utilising Windows Remote Management. Identifying a Remote Computer and Organizing an Activity: Organizing a Work Schedule The Web Shell is a part of the programme that runs on the server. Theft versus Production in the Execution of Signed Binary Proxies Using Rundll32 Kerberos Tickets for the event known as Kerberoasting are now available for purchase. The use of code signing in addition to other forms of trust control Compromisez la chaîne de fourniture du logiciel, la découverte de l'information sur le système, et la configuration du réseau du système: Unencrypted credentials include the likes of Internet Connection Cookies. Procedure Carried Out by the User: Malicious Link and Malicious File, Valid User Accounts and Domain Users, Web Services: Bidirectional Communication, and Windows-Management Instrumentation are some of the issues that are addressed in this section. [2]-[13]-[33]-[39]. And in terms of the malware, this (group APT29) used a package of malware including:

AdFind: is a free command-line inquiry device that can be utilized for gathering data from the Dynamic registry. Utilizing already stolen qualifications the assailant logged into a space controller and replicated devices into the %TEMP% catalog. Replicated devices included AdFind.exe (Dynamic Catalog count utility), a group script (Figure 2), and a duplicate of the 7-Zip chronicle utility [33]. the Adfind malware will be downloaded from all utilities and replicated to C:WindowsSysWOW64. The aggressor performed to have and organize surveillance utilizing built-in Windows commands. AdFind.exe was executed utilizing the already famous bunch script, which was created to pass the utility an arrangement of the entire commands that were utilized to gather data almost Dynamic Registry clients, frameworks, OUs, subnets, bunches, and believe targets. The yield from each command was spared to a person's content record nearby

the AdFind.exe utility. This handle was performed twice on the same space controller, 10 hours separated. Between executions of Adfind, the aggressor tried to get to multiple space controllers within the casualty environment, counting the one afterward utilized to convey Ryuk [10].

BoomBox: is a downloader mindful of executing another arranged component that has been utilized by APT29 since at slightest 2021. In a moment web journal post discharged Friday night, Microsoft gives points of interest on four modern malware families utilized by Nobelium in these later attacks. The four unused families incorporate an HTML connection named 'EnvyScout', a downloader known as 'BoomBox,' a loader known as 'NativeZone', and a shellcode downloader and launcher named VaporRage. Microsoft is following the BOOM.exe record within the ISO picture as 'BoomBox,' and states that it is utilized to download two scrambled malware records to the contaminated gadget from DropBox. After decoding the downloaded records, BoomBox malware directly takes action to spare them as AppData%MicrosoftNativeCacheNativeCacheSvc.dll, meanwhile,"%AppData%SystemCertificatesCertPKIPProvider.dll", in addition, execute them utilizing rundll32.exe [12]. NativeCacheSvc.dll is arranged to dispatch naturally when a client logs into Windows and is utilized to dispatch CertPKIPProvider.dll. As a last arrange, the BoomBox malware will assemble data approximately the Windows space encrypts the gathering data, hence, sends it to a farther server beneath the attacker's control. As the ultimate surveillance step, in the event that the framework is domain-joined, BoomBox executes an LDAP inquiry to accumulate information such as recognized title, SAM account title, then show the title of all space clients utilizing the channel (&(objectClass=user)(objectCategory=person)) it has been clarified by Microsoft [12].



```

public void BoomBox(string AccessName, string SavePath, byte[] Data)
{
    HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(this.ContentDomain + "/?files/upload");
    httpWebRequest.Timeout = 120000;
    httpWebRequest.Method = "POST";
    httpWebRequest.UserAgent = "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4268.1 Safari/537.36";
    httpWebRequest.Headers["Authorization"] = "Basic " + AccessName;
    httpWebRequest.ContentType = "application/octet-stream";
    string value = ("path": "" + SavePath + ",mode": "overwrite", "autorename": true, "mute": false, "strict_conflict": false);
    httpWebRequest.Headers["Content-Disposition"] = "form-data; name=\"data\"; filename=\"" + value + "\"";
    httpWebRequest.GetRequestStream().Write(Data, 0, Data.Length);
    httpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse();
    if (httpWebResponse.StatusCode != HttpStatusCode.OK)
    {
        return false;
    }
    string input = new StreamReader(httpWebResponse.GetResponseStream()).ReadToEnd();
    if (this.IsDownloadable(input))
    {
        this.PathLower_Match(input);
        this.ContentHash_Match(input);
        this.ContentSize_Match(input);
        return true;
    }
    return false;
}

// Token: 0x00000001 RID: 1
private string AppDomain = "https://api.dropbox.com/";
// Token: 0x00000002 RID: 2
private string ContentDomain = "https://content.dropbox.com/";
// Token: 0x00000003 RID: 3
private Regex PathLower = new Regex(@"path_lower:\s*\{([\s\S]*)}");
// Token: 0x00000004 RID: 4
private Regex ContentHash = new Regex(@"content_hash:\s*\{([\s\S]*)}");
// Token: 0x00000005 RID: 5
private Regex ContentSize = new Regex(@"size:\s*\{([\s\S]*)}");
// Token: 0x00000006 RID: 6
private Regex IsDownloadable = new Regex(@"is_downloadable:\s*\{([\s\S]*)}");

```

FIGURE 5. BoomBox downloads an encrypted file from Dropbox.

CloudDuke: is a very critical malware that was used by APT29 in 2015. APT29 used this malware to attack governments and private institutions over the world. And according to F-Secure, they mention that about this malware has seen the excursion of two modern augmentations to the Duke group's toolset, SeaDuke and CloudDuke [6]. Of these, SeaDuke could be a straightforward trojan made curiously by the truth that it's composed in Python. And indeed, more inquisitively, SeaDuke, with its built-in support for both Windows and Linux, is the primary cross-platform malware we have watched from the Duke gather. Whereas SeaDuke could be a single - though cross-platform - Trojan, CloudDuke shows up to be a whole toolset of malware components, or "arrangements" as the Duke bunch clearly calls them [7]. These components incorporate an interesting loader, downloader, and not one but two distinctive trojan components. CloudDuke moreover incredibly extends on the Duke group's utilization of cloud capacity administrations, particularly Microsoft's OneDrive, this malware is able to use command and control as well as the data exfiltration to stolen information. At last, a few of the later CloudDuke spear-phishing campaigns have born a striking likeness to CozyDuke spear-phishing campaigns from a year ago [6]- [7].

Cobalt Strike: this computer application promotes itself as an adversary role-playing simulation and is designed to mimic the post-exploitation behaviours of advanced risk actors as a commercially available, fully featured tool. Post-exploit capabilities of Cobalt Strike span the whole ATT&CK strategy range, all done in a single system. Cobalt Strike uses Metasploit and Mimikatz as well as other well-known tools to expand its claim capabilities [2].

CosmicDuke: Is used by APT29 since 2015. Found in 2014, CosmicDuke employs the ancient fashion Miniduke inserts from 2013 that are still around and are being utilized in dynamic campaigns that target governments and the private sector in different countries. After the 2013 presentation, the on-screen character behind Miniduke began utilizing another custom backdoor. It is one of the most critical Miniduke backdoors, it is able of taking different sorts of information. Although the Miniduke Well-suited on-screen character ceased its campaign, or at least decreased its escalation, within the starting of 2014 they once more continued assaults in full drive in early 2014 [16]. This time around we have taken note of changes in the way aggressors act and the instruments they utilize [16].

CozyCar: APT29 used this malware between 2010 and 2015. Backdoor components of malware may teach users how to download and run a variety of modules, each with a different purpose. As part of the CozyCar campaign utilised by the APT, stick phishing emails are used to deliver the payload from either a .zip record on a compromised site or through coordinate delivery as a link to the phish. The phishing interface was not dynamic at the time of our analysis. When the connected record is opened by a client, an executable file VT1/54 that has not been properly recognised is extracted. A self-extracting archive might be used as the first dropper (SFX). Upon execution, this executable file will drop a bait.wav file and an auxiliary dropper into the %TEMP% registry. In order to lure customers,

the CozyDuke compiles widely used genuine media recordings. Realistically, as an audio file of a female voice purporting to be that of a reporter looking for opinion is being played, the auxiliary dropper is working away in the background. APT29 using another set of critical malware such as EnvyScout, FatDuke, GeminiDuke, GoldFinder, GoldMax, HAMMERTOSS, ipconfig, LiteDuke, meek, Mimikatz, MiniDuke, NativeZone, Net, OnionDuke, PinchDuke, PolyglotDuke, POSHSPY, PowerDuke, PsExec, Raindrop, RegDuke, SDelete, Sibot, Sliver, SoreFang, SUNBURST, SUNSPOT, Systeminfo, Tasklist, TEARDROP, Tor, VaporRage, WellMail, wellness [18].

12- Axiom: Chinese actor of the threat For at least the last six years, As a result of our efforts, a total of 43,000 pieces of isolated Maxim equipment, including 180 of their most advanced implants, were uncovered and decontaminated. This study will elaborate on significant results that were previously uncovered. It may be to the advantage of state-backed players who pose a danger to be able to more easily exert influence over the private sector [19]. Saying danger might be a well-resourced, educated, and clever subdivision of a larger cyber covert operations organisation that has coordinated acts released over more than six years. Novetta is completely certain that the organization-tasking Saying is a part of the Chinese Insights Device when it comes to this particular aspect of the saying. This belief was backed to some extent by a second FBI flash that was sent to Infrared. This flash said that the performers are working in conjunction with the Chinese government. We've seen Axiom's operators at work in both public and private sector organisations with strategic economic interests, influencing conservation policy and, of course, energy policy, as well as developing cutting-edge information technology like integrated circuits, telecom equipment manufacturers, and so on. This is in reference to the treatment of individuals and groups that are seen as posing a threat to the stability of the

Chinese state, such as pro-democracy non-governmental organisations (NGO). - The final stages of operations, according to axiom, are dependent on command and control systems that have been hacked in order to target individuals from associated targeted groups. Malware is one of the numerous weapons that Axiom uses to assault vulnerable targets, and owing to the tremendous customisation it employs, it has the potential to live for months or even years at a time. The Zox family (ZoxPNG and ZoxRPC), the Hikit family, the Poison-Ivy/Darkmoon/Breut family, the Gh0st/Moudour/Mydoor family, the PlugX/Sogu/Kaba/Korplug/DestroyRAT family, the ZXShell/Sensode family, Hydraq/9002/Naid/Roarur/Mdmbot family, F It is probable that Novetta, in its capacity as the head of Operation SMN, is helping to facilitate a concerted effort on the part of private security businesses. When Operation SMN was first initiated, the primary objective was to carry out an interdiction operation against a modern and sophisticated danger to the performing arts community that was headed by the industry. This alliance is an example of the new method of interdiction, which is a more effective way of doing things than the previous method that was being used. [30]-[31] On October 14 and 28, 2014, the team eliminated malware, disclosed position markers, and provided open information in an effort to mitigate the risk presented by the group of on-screen characters. Due to the fact that they are a particularly dangerous group, we will refer to them as the Axiom for the sake of this essay. In the beginning, the primary objective of this project was to make use of the Facilitated Malware Destruction programme developed by Microsoft in order to facilitate the sharing of information generated by Novetta's malware decoder technology and to construct large dedication markings for the Hikit malware family. This partnership between Novetta and Microsoft is going to result in the release of a malicious software removal tool (MSRT) that will first focus on the Hikit malware family. The initial few cycles of data sharing and signature

refinement that were conducted by Microsoft and Novetta demonstrated that involving additional industry partners might potentially offer a bigger test set for the purposes of collection, analysis, and action. As a consequence of this, the association developed into a very limited set of competent organisations that were able to make an overt contribution to the CME effort. As the operational breadth increased, the focus switched away from the Hikit malware family and toward attempts to attack the whole spectrum of related tools and malware capabilities that had been targeted in the past. This occurred as a result of the expansion of the operational width. As a consequence of this, the team came to the conclusion that the best strategy would be to take an all-encompassing approach. They would rely on the MSRT's capabilities for detection and eradication, while also using Microsoft's Infection Data Organization to share their findings with other businesses [32]. As a result of this, they came to the conclusion that 64 trusted industry partners located in 22 different countries may access and utilise extremely sensitive data for their own objectives as well as to protect the safety and security of their consumers. Individuals from Operation SMN were able to design and carry out a worldwide debasement campaign, during which they were successful in identifying the Chinese state-sponsored danger performer who has targeted and abused people all over the world. According to Novetta, the only way to successfully tackle this threat is by using a unified approach such as the one devised under Operation SMN, which brought together varied private sector viewpoints and capabilities. Novetta is certain that in the not-too-distant future, other businesses in the industry will follow a strategy similar to theirs. APT Can conduct Exfiltration

An APT, or advanced persistent threat, is a category of malware that is characterized by its ability to evade detection and remain dormant within a network for an extended period of time. Once activated, the APT can launch devastating attacks and exfiltrate sensitive data

from the network. The recent WannaCry ransomware attacks are a prime example of an APT in action. Advanced Persistent Threat (APT) groups are known for their ability to silently exfiltrate data from organizations for long periods [2]- [21]. A recent study showed that the average lifespan of an APT group is 8 months, compared to the 36 months it takes for

other malware to be discovered. This means that APTs have the potential to do much more damage than other types of malwares, as they often fly under the radar for long periods of time. we have designed this fellow to describe the APT attack after gain access to the infrastructure [21].

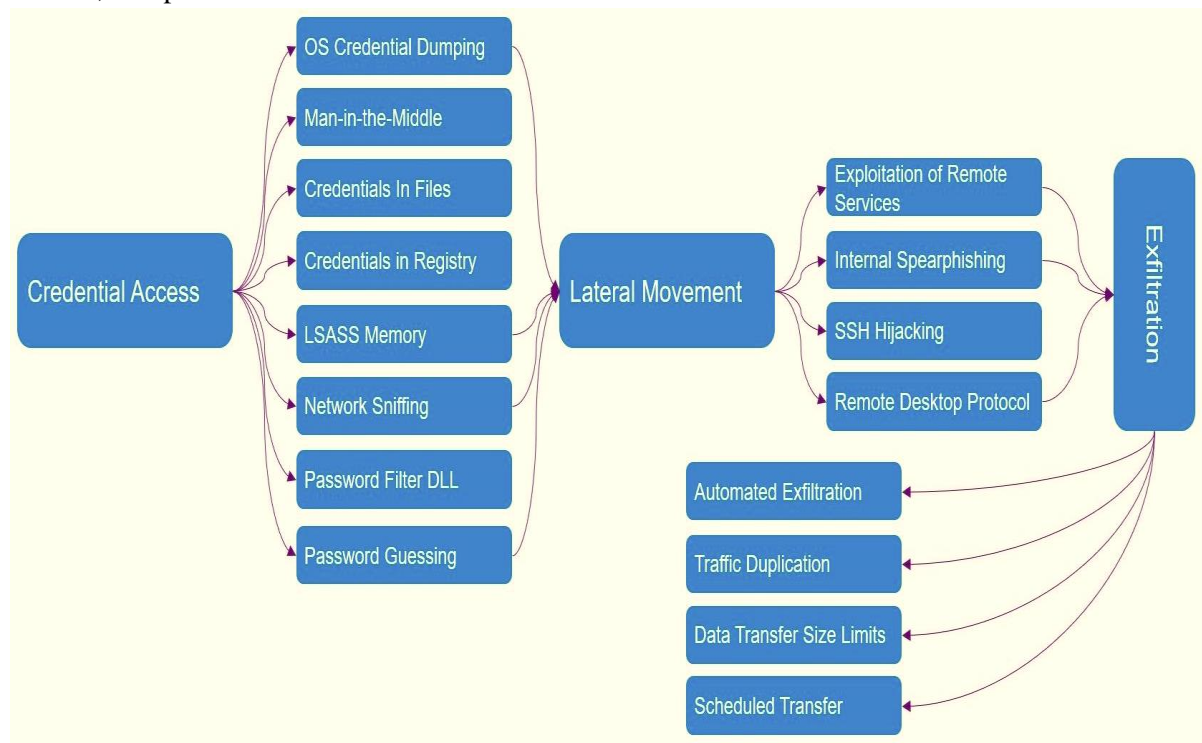


FIGURE 6. how APT able to conduct Exfiltration after gain access [21].

IV. THREAT INTELLIGENCE

Threat intelligence is a type of data that is created as part of a threat management program [45]. It can include information on the threats faced by an organization, how those threats are realized, the impact of those threats, and the mitigation strategies used to protect against them [46]. Threat intelligence is also valuable because it can provide insights into how threat actors work and what methods they use. This information helps organizations to better defend themselves against attack, as well as to identify potential vulnerabilities that could be exploited [47]. Cybercrime is a reality that all businesses must face. It's no longer a question of if your company will be targeted, but when. And the impact of a data breach can be devastating, costing an organization an average of \$3.5

million per incident. Threat intelligence is one weapon in your cyber defense arsenal. Threat intelligence is the process of identifying, collecting, analyzing, and sharing information about known and suspected cyber threats [48]. When used correctly, it can help you better protect your data. There's a reason business are willing to shell out big bucks for threat intelligence (TI) these days. And that's because TI is one of the most effective ways to protect an organization from cyberattacks. But what is threat intelligence? Simply put, it's information about potential or actual threats to an organization's security, collected and analyzed by security professionals [49]. And why is it so important? Because it gives organizations the ability to thwart attacks before they happen. Threat intelligence is the process of understanding an organization's adversaries and

their tactics, techniques, and procedures. This understanding helps organizations protect themselves against known threats and anticipate future threats. Threat intelligence is a vital part of any cybersecurity strategy and should be tailored to meet the specific needs of an organization [49]. By using threat intelligence, businesses can improve their cybersecurity posture, reduce the risk of data breaches, and improve their overall security posture. While firewalls and antivirus software can help, they're no longer enough in the face of determined and sophisticated cyber threats. That's where threat intelligence comes in. Threat intelligence is the practice of gathering information about potential cyber threats and vulnerabilities and using that information to inform security decisions and protect against attacks. It's an important tool in the fight against cyber-attacks. we recommend the organizations to use threat intelligence to detect and predict APT attacks [50].

V. CONCLUSIONS

This paper presents an anatomy of Chinese APT groups, Meanwhile, the tactics and tactics used, as well as the malware used to attack governments and private institutions around the world. In the same context, this paper deals with the importance of threat intelligence in the process of anticipating and reducing the damage of the attack by understanding the methods and methodologies used by APT at the time of the attack, hence suggesting solutions to mitigate each tactic through mapping it to MITRE ATT&CK. 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.

VI. ACKNOWLEDGEMENT

The Department of Internal Security at Rabdan Academy provided financial and emotional assistance for the writers to finish this work, and the authors are quite grateful to them. In addition, we would like to express our heartfelt gratitude and appreciation to all the reviewers and auditors of this study for their useful comments and recommendations, which

enhance the presentation of our research endeavour in a fantastic manner that helps the community and researchers alike.

REFERENCES

1. Alharbi, F., Chang, J., Zhou, Y., Qian, F., Qian, Z., & Abu-Ghazaleh, N. (2019, April). Collaborative client-side DNS cache poisoning attack. In IEEE INFOCOM 2019-IEEE Conference on Computer Communications (pp. 1153-1161). IEEE.
2. 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.
3. Li, F., Li, Q., Zhang, J., Kou, J., Ye, J., Song, W., & Mantooth, H. A. (2020). Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network. *IEEE Transactions on Power Electronics*, 36(3), 2495-2498.
4. Nazarov, A. N., Sychev, A. K., & Voronkov, I. M. (2019, June). The Role of Datasets when Building Next Generation Intrusion Detection Systems. In 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) (pp. 1-5). IEEE.
5. Hassan, W. U., Bates, A., & Marino, D. (2020, May). Tactical provenance analysis for endpoint detection and response systems. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 1172-1189). IEEE.
6. Ajmal, A. B., Shah, M. A., Maple, C., Asghar, M. N., & Islam, S. U. (2021). Offensive security: Towards proactive threat hunting via adversary emulation. *IEEE Access*, 9, 126023-126033.
7. Saleem, Shahnaz, Sana Ullah, and Kyung Sup Kwak. "A study of IEEE 802.15. 4 security framework for

- wireless body area networks." *Sensors* 11.2 (2011): 1383-1395.
8. Karuna, P., Hemberg, E., O'Reilly, U. M., & Rutar, N. (2021). Automating Cyber Threat Hunting Using NLP, Automated Query Generation, and Genetic Perturbation. *arXiv preprint arXiv:2104.11576*.
 9. 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.
 10. Golushko, A. P., & Zhukov, V. G. (2020, January). Application of Advanced Persistent Threat Actors Techniques for Evaluating Defensive Countermeasures. In *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIconRus)* (pp. 312-317). IEEE.
 11. Hong, S., Kim, K., & Kim, T. (2019). The Design and Implementation of Simulated Threat Generator based on MITRE ATT&CK for Cyber Warfare Training. *Journal of the Korea Institute of Military Science and Technology*, 22(6), 797-805.
 12. Enoch, S. Y., Huang, Z., Moon, C. Y., Lee, D., Ahn, M. K., & Kim, D. S. (2020). HARMer: Cyber-attacks automation and evaluation. *IEEE Access*, 8, 129397-129414.
 13. Miller, D., Alford, R., Applebaum, A., Foster, H., Little, C., & Strom, B. (2018). Automated adversary emulation: A case for planning and acting with unknowns. MITRE CORP MCLEAN VA MCLEAN.
 14. Toorani, M. (2015, January). On vulnerabilities of the security association in the IEEE 802.15. 6 standard. In *International conference on financial cryptography and data security* (pp. 245-260). Springer, Berlin, Heidelberg.
 15. Gianvecchio, S., Burkhalter, C., Lan, H., Sillers, A., & Smith, K. (2019, October). Closing the gap with APTs through semantic clusters and automated cybergames. In *International Conference on Security and Privacy in Communication Systems* (pp. 235-254). Springer, Cham.
 16. Taofeek, O. T., Alawida, M., Alabdulatif, A., Omolara, A. E., & Abiodun, O. I. (2022). A Cognitive Deception Model for Generating Fake Documents to Curb Data Exfiltration in Networks During Cyber-Attacks. *IEEE Access*.
 17. Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. *Heliyon*, 4(11), e00938.
 18. Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Umar, A. M., Linus, O. U., ... & Kiru, M. U. (2019). Comprehensive review of artificial neural network applications to pattern recognition. *IEEE Access*, 7, 158820-158846.
 19. Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital forensics: review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems*, 14(2), 346-376.
 20. Mohamed, N. A., Jantan, A., & Abiodun, O. I. (2018). An improved behaviour specification to stop advanced persistent threat on governments and organizations network. In *proceedings of the International MultiConference of Engineers and Computer Scientists* (Vol. 1, pp. 14-16).
 21. Mohamed, N. (2022). Study of bypassing Microsoft Windows Security using the MITRE CALDERA Framework. *F1000Research*, 11(422), 422.
 22. Mohamed, N. A., Jantan, A., & Omolara, A. E. Mitigation of Cyber

- Terrorism at ATMs, and Using DNA, Fingerprint, Mobile Banking App to withdraw cash (Connected with IoT).
23. Golushko, A. P., & Zhukov, V. G. (2020, January). Application of Advanced Persistent Threat Actors Techniques for Evaluating Defensive Countermeasures. In 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIconRus) (pp. 312-317). IEEE.
 24. Reddy, B. H. K., & Anitha, K. (2022, February). A Comparative Analysis for Measuring Accuracy in Recognizing Hand Gestures using Feedforward Neural Network and CNN Method. In 2022 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-8). IEEE.
 25. Mohamed, Nachaat AbdElatif, Aman Jantan, and Abiodun Esther Omolara. "Mitigation of Cyber Terrorism at ATMs, and Using DNA, Fingerprint, Mobile Banking App to withdraw cash (Connected with IoT)."
 26. Mohamed N. Holistic Approach Drone System (HADS) [version 1; not peer reviewed]. *F1000Research* 2022, 11:19 (poster) (<https://doi.org/10.7490/f1000research.1118903.1>).
 27. Sen, Ö., van der Velde, D., Peters, S. N., & Henze, M. (2021). An Approach of Replicating Multi-Staged Cyber-Attacks and Countermeasures in a Smart Grid Co-Simulation Environment. *arXiv preprint arXiv:2110.02040*.
 28. Brangetto, P., & Veenendaal, M. A. (2016, May). Influence cyber operations: The use of cyberattacks in support of influence operations. In 2016 8th International Conference on Cyber Conflict (CyCon) (pp. 113-126). IEEE.
 29. Naveen, S., Puzis, R., & Angappan, K. (2020, September). Deep Learning for Threat Actor Attribution from Threat Reports. In 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP) (pp. 1-6). IEEE.
 30. Perry, L., Shapira, B., & Puzis, R. (2019, July). No-doubt: Attack attribution based on threat intelligence reports. In 2019 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 80-85). IEEE.
 31. Geiger, M., Bauer, J., Masuch, M., & Franke, J. (2020, September). An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems. In 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (Vol. 1, pp. 1537-1543). IEEE.
 32. Siadati, H., Saket, B., & Memon, N. (2016, October). Detecting malicious logins in enterprise networks using visualization. In 2016 IEEE Symposium on Visualization for Cyber Security (VizSec) (pp. 1-8). IEEE.
 33. Toker, F. S., Akpınar, K. O., & ÖZÇELİK, İ. (2021, June). MITRE ICS Attack Simulation and Detection on EtherCAT Based Drinking Water System. In 2021 9th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.
 34. Siadati, Hossein, Bahador Saket, and Nasir Memon. "Detecting malicious logins in enterprise networks using visualization." In 2016 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1-8. IEEE, 2016.
 35. Yin, M., Wang, Q., & Cao, M. (2019, October). An Attack Vector Evaluation Method for Smart City Security Protection. In 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (pp. 1-7). IEEE.

36. 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.
37. Nisioti, A., Loukas, G., Laszka, A., & Panaousis, E. (2021). Data-driven decision support for optimizing cyber forensic investigations. *IEEE Transactions on Information Forensics and Security*, 16, 2397-2412.
38. Noor, U., Anwar, Z., & Rashid, Z. (2018, July). An Association Rule Mining-Based Framework for Profiling Regularities in Tactics Techniques and Procedures of Cyber Threat Actors. In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 1-6). IEEE.
39. Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P., & Gourisetti, S. N. G. (2020, October). Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping. In 2020 Resilience Week (RWS) (pp. 106-112). IEEE.
40. Diffenderfer, P. A., Baumgartner, D. M., Long, K. M., Pertsch, C. F., & Iacobucci, S. D. (2020, October). Authentication and Authorization Challenges for Controller-Pilot Information Exchange Using Mobile Devices. In 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC) (pp. 1-8). IEEE.
41. 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.
42. Fujimoto, M., Matsuda, W., & Mitsunaga, T. (2018, November). Detecting abuse of domain administrator privilege using windows event log. In 2018 IEEE Conference on Application, Information and Network Security (AINS) (pp. 15-20). IEEE.
43. Niakanlahiji, A., Wei, J., & Chu, B. T. (2018, December). A natural language processing based trend analysis of advanced persistent threat techniques. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 2995-3000). IEEE.
44. Wang, W., Zhang, X., Dong, L., Fan, Y., Diao, X., & Xu, T. (2020, October). Network Attack Detection based on Domain Attack Behavior Analysis. In 2020 13th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI) (pp. 962-965). IEEE.
45. Al-Hawawreh, M., Moustafa, N., Garg, S., & Hossain, M. S. (2020). Deep learning-enabled threat intelligence scheme in the Internet of Things networks. *IEEE Transactions on Network Science and Engineering*, 8(4), 2968-2981.
46. Mavroeidis, V., & Bromander, S. (2017, September). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In 2017 European Intelligence and Security Informatics Conference (EISIC) (pp. 91-98). IEEE.
47. Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., ... & Shakarian, P. (2016, September). Darknet and deepnet mining for proactive cybersecurity threat intelligence. In 2016 IEEE Conference on Intelligence and Security Informatics (ISI) (pp. 7-12). IEEE.
48. Deliu, I., Leichter, C., & Franke, K. (2017, December). Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks. In 2017

- IEEE International Conference on Big Data (Big Data) (pp. 3648-3656). IEEE.
49. Gao, Y., Xiaoyong, L. I., Hao, P. E. N. G., Fang, B., & Yu, P. (2020). Hincti: A cyber threat intelligence modeling and identification system based on heterogeneous information network. *IEEE Transactions on Knowledge and Data Engineering*.
50. 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.