Investigating Initial Access Strategies and Malware Deployment Tactics Used by Iranian Advanced Persistent Threat Groups

Ryan Simons
Marymount University
Department of Cybersecurity
Arlington, VA, U.S.
rps79099@marymount.edu

2023 IEEE International Conference on Big Data (BigData) | 979-8-3503-2445-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/BigData59044.2023.10386701

Abstract—**In the domain of cyber threats, Iran is listed among the top four concerns for the United States. Beyond its nuclear potential, Iran commands a substantial cyber force linked to at least 11 Advanced Persistent Threats (APTs), responsible for a wide range of cyber attacks targeting government, healthcare, infrastructure, and essential services like power. Mapping APT threats is crucial in the Cyber Threat Intelligence (CTI) field, as network defenders must have actionable knowledge to implement defenses. Linking these Tactics, Techniques, and Procedures (TTPs) and common attack vectors is one step toward this goal. There is a gap in existing research identifying similarities and common tactics shared among Iran APT malware and initial access vectors. This research examines the Advanced Persistent Threats (APTs) attributed to Iran, focusing on historically documented and currently active groups, focusing on their malware and TTPs.**

Index Terms—**APT, Advanced Persistent Threat, Iran, Threat Actor, Cyber, Malware**

I. Introduction

Advanced Persistent Threat (APT) groups, allegedly linked to the Iranian government [1], exhibit substantial resource capabilities and demonstrate operational patterns corresponding with the MITRE ATT&CK Framework. These Iran-attributed APTs will be the main focus of the research to discover new correlations between their initial access approaches and gain insight into how their malware is used in the Cyber Kill Chain. A pivotal concern for cybersecurity experts is effectively countering these APT threats. Some situations will be addressed by identifying shared characteristics and potential indicators of compromise. The ultimate aim is to elucidate commonalities among the APTs' Tactics, Techniques, and Procedures (TTPs) to reveal broader patterns that may inform defensive strategies.

II. Research Objective

The objective of the research is to find commonalities in the approach that Iran attributed APTs use when gaining initial access into an organization. Throughout the research, a goal is to identify the malware associated with the APT groups and designate where they occur in the cyber kill chain.

III. Methodology

The methodology of this report involves extensive open-source research to gather information from various sources and find common trends among the APT groups. The sources that will be used include scholarly articles and journals from scholar.google.com and Proquest. Open-source information will be collected from various cybersecurity vendors, including Kaspersky, Unit 42 (Palo Alto Threat Intelligence Team), Talos (Cisco Intelligence Group), Microsoft Threat Intelligence, ClearSky Security, and some government agencies, including the Cybersecurity & Infrastructure Security Agency (CISA) and U.S. Cyber Command (CYBERCOM). Information will be collected and reported in the ”related work” section to facilitate the identification of shared trends of initial access vectors and malware functionality. Identifying such commonalities will help discern potential collaborations between APT groups or shared TTPs.

IV. Background

A. Why Iran?

Iran is featured in this report as one of the United States' principal cyber adversaries, forming part of the ”*Big Four*” representing the most significant cyber threats [2]. This analysis is the initial installment in a series that will delve into the cyber capabilities of each of these adversaries through their APT activities. Understanding the tactics of APT groups associated with Iran may aid in the determination of how they might conduct their cyber offensive operations. Subsequent reports will address Russia, China, and North Korea, allowing for a comparative analysis of the cyber operations of the Big Four's APTs.

B. What is an Advanced Persistent Threat?

NIST defines an APT as *”an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and* *deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives".* [3]

C. Threat Actor Naming Scheme

Most of these groups have multiple names associated with them, and there is a reason why. During a breach or incident, an investigation group will assign a code name based on the attack's characteristics and observed activity [4]. The code name might refer to an existing activity cluster if there is sufficient overlap in observed activities. For example, an investigation may have been conducted on an attack and a group named the activity cluster Gold Fritter. If another incident is investigated by another group, they may give the entity another name, such as Rabid Penguin. These names are given by different groups investigating specific details and activity of the Activity Clusters. These attributes may belong to the same threat actor; however, each investigator has different visibility on activities [4]. Thus the same activity cluster can have multiple names assigned by different investigators [5]. In short, different companies look at different endpoints and logs to derive their information. The term alias for these APT groups has become deprecated, and these activity groups are now being observed as "*activity clusters*"

The Diamond Model is typically used by organizations when determining if the activity clusters will be assigned a new name by these entities. The diamond model has four main components, as shown in Figure 1 below, consisting of an adversary, victim, infrastructure, and capability [6]. When an intrusion occurs, the entity that investigates the breach will typically map the incident against these four characteristics and the meta-features seen in Figure 1. If the examined threat actor's activity overlaps with known activity clusters but with additional activity that was not seen before, a new name is assigned to the same cluster by the investigator. [6].

D. Characteristics of an APT

Chen et al. [7] identified four key characteristics that can pinpoint whether an attacking entity is an APT or a traditional attacker. These four characteristics are that APTs have specific targets with clear objectives, are highly organized and well-resourced, conduct long-term campaigns with repeated attempts, and use stealth and evasive techniques [7]. These will be elaborated on in the following sections.

1) Specific Targets and Clear Objectives: APTs always have identified targets in which they will attack. The targeting portion can take days, weeks, months, or even years before the initial attack is conducted [7]. When these targets are identified, there is always a motivation for either sensitive data extraction, government affiliation, or political gain. The APT will always have a defined objective they are trying to achieve when conducting their attacks and typically will not stop until it is attained [7]. According to Mandiant, APTs have changed their top 10 targeted industries over the past eight years; however, most of the same industries still appear in the top ten. (See Table 1).

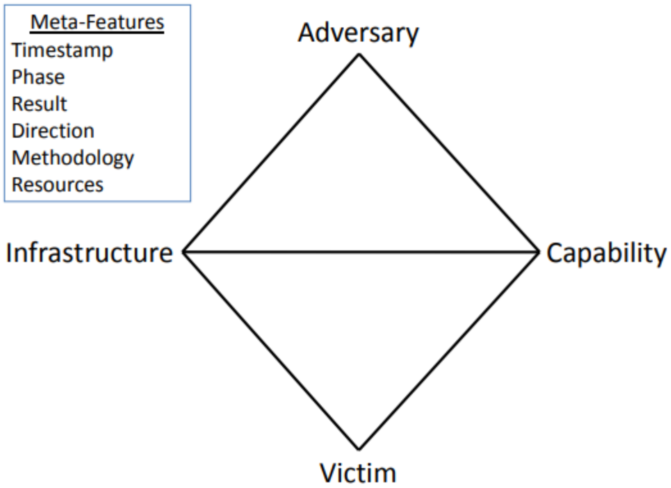

Fig. 1: Diamond Model of Intrusion Analysis as presented by Caltagirone et al. [6]

Mandiant Top 10 Industries Targeted by APTs 2013 vs 2021		
Ranking	2013	2021
1	Education	Business & Professional
2	Finance	Finance
3	High-Tech	Healthcare
4	Government	Retail & Hospitality
5	Consulting	High-Tech
6	Energy	Government
7	Chemical	Transportation and Logistics
8	Telecommunications	Construction & Logistics
9	Healthcare	Construction & Engineers
10	Aerospace	Telecommunications

TABLE I: Mandiant Top 10 Industries Targeted by APTs [8]

2) Highly Organized and Well-Resourced: One significant difference between a nation-state-sponsored APT and a casual hacker is the level of organization and resources available to the team. APTs have highly skilled cyber operators who can conduct organized missions and assessments dealing significant consequences to their targets. These individuals can be members of the government, military, or hired as freelance mercenaries to support the cause [9].

3) Conduct Long-Term Campaigns with Repeated Attempts: Traditional attackers will attempt to find systems that are considered "*low-hanging fruit*" or easily exploitable instead of taking the effort to break into hardened systems [7]. APTs do not have the same methodology and TTPs as the standard attacker. If an APT selects a target, the cell will not stop until it gains access to that objective. If their first attempt at exploitation does not work, the technique changes and another attempt will be made [7]. This will continue until the system or network of interest is compromised. The APT cell can work on the same target for days, weeks, months, or even years [7]. After compromise, an APT may establish a persistent cyber operation (PCO) to keep themselves in the network and continually exfiltrate information on their adversary.

4) Stealth and Evasive Techniques: How TTPs are conducted differs between an APT and traditional attackers. Traditional attackers may go into an engagement, creating a lot of noise on a network to collect as much information or data as possible before they either pull out or get caught. APTs are tedious about how they move on a network. All their moves are calculated to access their target and complete their mission. They use a combination of zero-day exploits, which has a low chance to get caught by endpoint solutions or signature-based antivirus [10]. If the APT cell has access to the intelligence cells of the military and government, they may also have access to many different zero-days. APTs will attempt to remain hidden while traversing a network, as they may have to be there for years to complete their objective without raising alarms.

E. Cyber Kill Chain

A cyber kill chain is a tool that can be used by intelligence and threat modeling personnel to identify a series of steps in the cyber attack process. This tool can show an attack's stages and how one can build upon another. Mandiant has published a targeted attack life cycle, which is their version of the cyber kill chain, as shown in Figure 2 [11]. The APT cells are highly organized and know how to remain hidden. APTs operate systematically, following a series of eight phases to infiltrate, exploit, and control network resources. These phases include initial reconnaissance, initial compromise, establishing a foothold, escalating privileges, lateral movement, maintaining presence, internal reconnaissance, and mission completion [11]. Notably, four phases; maintaining presence, escalating privileges, internal reconnaissance, and lateral movement—are recurrent, ensuring continuous command and control over additional systems within a network [11].

V. Related Work

Prominent entities like Mandiant, Unit 42, Talos, FireEye, CISA, USCYBERCOM, and MITRE have significantly contributed to the existing body of knowledge for the world's APT groups. MITRE's ATT&CK Framework, in particular, has emerged as a comprehensive resource, attributing specific attacks and methodologies to various APTs [12]. This paper strives to present a cohesive synthesis of existing research, providing a unified and comprehensive view of Iran-attributed APTs, their initial access vectors, and malware used during their campaigns.

A. Activity Cluster 1

a) Associated Activity Clusters: APT-33, Elfin, Holmium, Peach Sandstorm, Magnallium, and Refined Kitten

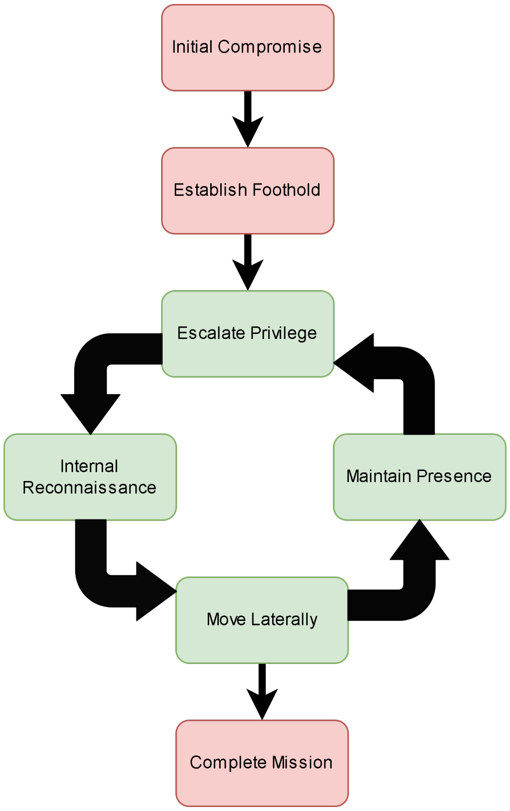

Fig. 2: Mandiants Targeted Attack Life Cycle [11]

b) Overview: These activity clusters are known to have destructive campaigns in the aviation and energy sectors throughout the United States, Saudi Arabia, and South Korea [13]. The groups were first observed in 2013 and had activity in early 2023 when conducting password spray attacks, according to Microsoft Threat Intelligence [14].

c) Initial Access: These clusters primarily target the aviation and energy industry, with the most used tactic to gain initial access being spear phishing using .hta files [15]. Showcasing the intricacy of the group, the phishing emails would be tailored to aviation and would lure the victims in this way. Within the email would be malicious links that would forward the victim to legitimate job postings; however, embedded code would be downloaded and run in the background to establish a backdoor [15].

d) Associated Malware: Malware associated with the group includes SHAPESHIFT, DROPSHOT, STONEDRILL, TURNEDUP, NANOCORE, ALFA Shell, PoshC2, POWERTON and NETWIRE [16]. DROPSHOT is a custom dropper program developed by APT-33 that can deliver additional malware to systems. DROPSHOT has been identified to drop the TURNEDUP backdoor that APT-33 has created, allowing for full command and control (C2) of an infected host [17]. The SHAPESHIFT malware is a known malicious wiper program that can completely wipe the hard drives of infected systems. DROPSHOT has not been directly linked to dropping the SHAPESHIFT program directly; however, there have been references to "*samples*" of the DROPSHOT dropper delivering SHAPESHIFT [18]. Speculatively, this could be an updated version of DROPSHOT that is not yet signatured by antivirus(AV) organizations or another threat entity has received DROPSHOT and has not modified the code enough to give it enough distinction as a new custom dropper. TURNEDUP is a custom backdoor used by APT-33 that allows remote access into an infected machine [15]. The primary use of this backdoor is for uploading and downloading files, creating reverse shells, taking screenshots, and gathering information on a network. Dubbed "*STONEDRILL*" from Kaspersky, this malware is another disk-wiping variant that has a very similar resemblance to SHAMOON [19]. An additional backdoor used by APT-33 is NANOCORE, which is publicly available for download on GitHub. This tool is a backdoor Remote Access Trojan (RAT) that comes fully backed with a plugin framework [18], [20]. ALFA Shell is used primarily in APT-33s initial access phishing campaigns [17]. This malware is again open-source and publicly available for download on GitHub [21]. As mentioned previously, the phishing emails would reference specific job opportunities within the aviation sector and would provide information such as the job description, salary and provide a link to a spoofed employment website [21]. Clicking the malicious link would execute the ALFA Shell and provide a reverse shell for the attacker to operate from. The last notable malware APT-33 utilizes is NETWIRE. This malware runs in the initial reconnaissance portion of the cyber kill chain. NETWIRE is a backdoor that steals credentials from the local machine executed on and also has most of the standard features of a typical backdoor [15].

B. Activity Cluster 2

a) Associated Activity Clusters: APT-34, Oil Rig, COBALT GYPSY, Helix Kitten, GreenBug, IRN2, Twisted Kitten, Crambus, Chrysene, TA452, ATK 40, ITG13

b) Overview: Just like activity cluster 1, these activity clusters are known for their destructive campaigns in the Middle East and have been active since 2014 [22]. HiveForce Labs has reported a recent development attributed to the activity cluster called CRAMBUS that began in August 2022 and has been active into 2023 [23]. Trend Micro has also attributed an attack occurring in the same time frame that appears to be different as the attackers were targeting mail servers to exfiltrate sensitive email contents [24]. Two instances of attribution to these threat groups show that this APT is still active today.

c) Initial Access: The most recent initial access that APT-34 has used is a phishing campaign as part of the CRAMBUS campaign that consisted of a Microsoft Word document embedded with a malicious macro [23]. The macro would create one Visual Basic Script (VBS) and two PowerShell scripts, temp.ps1 and Script.ps1 [23]. Historically, these threat groups utilized spear-phishing with macro-enabled .rtf files that exploited CVEs (CVE-2017-11882 & CVE-2017-0199) as a typical initial access vector [25].

d) Associated Malware: The most recent malware attributed to these groups is the .NET dropper "MrPerfectInstaller.exe" that downloads and writes two .dll files and two .exe files to disk [24]. The filenames are PsgFiler.dll, DeviceSrv.exe, Microsoft.Exchange.Webservices.dll, and DevicesSrv.exe [24]. Previously used malware consists of POWBAT, POWRUNNER, ZEROCLEARE, DNSPIONAGE, PICKPOCKET, VALUEVAULT, and LONGWATCH. POWBAT is a backdoor program that gets delivered by phishing email and, once executed, allows for C2 to be established back to the attacker. APT-39 has also been attributed to this malware with slight variations [26]. POWRUNNER was a PowerShell-based backdoor first seen in 2017 as reported by Mandiant [25]. ZEROCLEARE is a wiper malware that closely resembles the SHAMOON malware as it overwrites the Master Boot Record (MBR) of an operating system and also utilizes the same "ElDOS RawDisk" tool to complete the wipe [27]. DNSPIONAGE is a campaign that was conducted in 2018 that consisted of a phishing campaign that lured victims in with job opportunities via LinkedIn and would deliver macro embedded documents according to Checkpoint Research. [28]. The DNSESPIONAGE malware was a reconnaissance tool to gather information using the username, hostname, and the systeminfo commands. The tool would then store the collected data in multiple files in the %UserProfile%ȯracleServices directories [29]. This tool could support DNS and HTTP connections and use these protocols to exfiltrate the collected data [29]. PICKPOCKET is a browser theft tool that FireEye has been tracking since 2018. There are two indicators of compromise with this tool, and they are PE86.dll and PE64.dll, which the malware uses to collect the information [30]. VALUEVAULT is another credential-stealing tool that attempts to scrape the Windows Credential Manager for stored credentials [30]. LONGWATCH is a keystroke monitoring tool that will collect a user's keystrokes and store them in the Windows Temp directory as log.txt [30].

C. Activity Cluster 3

a) Associated Activity Clusters: APT-35, Charming Kitten, Mint Sandstorm, Phosphorus, Newscaster, Saffron Rose, BadBlood, Magic Hound, COBALT ILLUSION, TA453, ITG18

b) Overview: According to Microsoft Threat Intelligence, these activity clusters are still active in 2023 and have been conducting tradecraft advancements in their n-day capabilities [31]. The threat groups have been tracked back to operations in 2014, according to MITRE [32].

c) Initial Access: These threat clusters have used phishing via false "Google Drive" links to lure victims into giving credentials. The malicious link sent to the victim brings them to a false Google page where the user is prompted to use their login credentials [33]. Another method APT-35 used was a deception campaign in which an email to the victim would state numerous advertisement emails had come from the victim, and they could click the link to review [33]. The third case involved an email from a supposed colleague asking for a review of the article they are working on [33]. The threat actor has recently been noticed using spear-phishing techniques in which the victims are being lured by an interview request which is a change from their mass mailing techniques in the past [34].

d) Associated Malware: Malware associated with the group includes Powerless, HAVIJ, Memento, and Bitlocker. The Powerless malware is a PowerShell backdoor that runs in a .NET context whose goal is to compromise Microsoft Exchange servers and establish as an agent to the C2 platform [35]. This malware can download and execute additional malware, execute commands on the server, keylog, and has an encrypted tunnel with the C2 server [35]. A link has been established between APT-35 and the threat group Memento as the Powerless malware shares the same google.onedriver-srv[.]mil domain as them [36]. HAVIJ is a tool developed to exploit SQL injection vulnerabilities automatically. The tool has been used by other activity clusters such as Magic Hound, establishing that the tool has been dispersed throughout Iran threat actors [37]. Bitlocker is a Microsoft tool that encrypts entire volumes or disks with a password and can be used on ransomware operations. An APT-35 subgroup coined "*Nemesis Kitten*" has used Bitlocker to encrypt victim hard drives [38].

D. Activity Cluster 4

a) Associated Activity Clusters: APT-39, ITG07, RemixKitten, Chafer

b) Overview: These activity clusters have been operating since at least 2014 and targeting multiple industry sectors. The clusters have targeted multiple countries, including Iran, Asia, Africa, Europe, and North America, to track individuals that pose a threat to the Iranian Ministry of Intelligence of Security [40].

c) Initial Access: The threat groups have used spear phishing that leverages the POWBAT backdoor mentioned with activity cluster 2. The APT group would create malicious macro-enabled attachments in the emails to gain initial access when opened [39]. The threat actor has also exploited public-facing web servers to gain initial network footholds. The last known vector displayed by these threat groups is using prior stolen credentials to authenticate to external Outlook Web Access (OWA) [39]

d) Associated Malware: As mentioned previously, these threat actors have leveraged a variant of the POWBAT backdoor malware similar to activity cluster 2 to gain initial access and communicate to their C2 infrastructure. Two other backdoor programs associated with APT-39 are SEAWEED and CACHEMONEY; however, there is little documentation on these two programs [41].

E. Activity Cluster 5

a) Associated Activity Clusters: APT-42, Crooked Charms

b) Overview: Activity cluster 5, which is composed of APT-42 and Crooked Charms was first seen by security researchers in 2015. These groups were closely attributed to the activity cluster known as APT-35, which has also been attributed to Iran [42]

c) Initial Access: Through research conducted by Picus Security, it was determined that sophisticated spear phishing attacks were attempted to conduct surveillance for the Iranian regime's interest [43]. In one such case in 2022, the attacker tried to masquerade as a vaccinologist from Oxford University and attempted to persuade an individual they would receive a report on proprietary vaccine information that was supposedly recovered from Chinese hackers, and the individual was needed to verify the contained data [43].

d) Associated Malware: These threat groups have developed two pieces of malware that target Android mobile devices: VINETHORN and PINEFLOWER [44]. VINETHORN was designed to be a C2 server for Android mobile, while PINEFLOWER was a surveillance operation in an Android application. Throughout the analysis on PINEFLOWER by Emiel Haeghebaert from FireEye, it was found that both PINEFLOWER and identified malicious files from threat actor Corrupt Kitten were the same (files included WhatsApp.apk and classes.dex) [45]. The PINEFLOWER malware communicates to the C2 server via HTTP POST request and utilizes the Android/.data/_gsc98647a3 directory for storage before exfiltrating the data. BROKEYOLK is a custom .NET backdoor that was developed to maintain persistence in the network [46]. This malware, once executed, downloads C2 infrastructure to the victims machine and uses a Simple Object Access Protocol (SOAP) application programming interface (API) request to connect back to the C2 server [46]. TAMECAT is a PowerShell backdoor used by APT-42 in the past and allows for credential harvesting of multi-factor codes [46]. The TAMECAT malware previously has been delivered via an embedded macro document that downloads and executes the program [44].

F. Activity Cluster 6

a) Associated Activity Clusters: Rampant Kitten

b) Overview: Rampant Kitten is a lone activity cluster first observed in the wild in 2014 and last seen in 2020. It has been attributed by Checkpoint Research to target expatriates and dissidents to the Iranian Regime as their primary focus [47].

c) Initial Access: Initial access methods for Rampant Kitten consisted of a Telegram phishing campaign targeted at Android devices belonging to individuals suspected of being opposed to the Iranian regime [47]. The document leveraged for this campaign was a template that allowed for remote loading of content that the attackers modified to execute a batch script and reach out to afalr-sharepoint[.]com [47].

d) Associated Malware: Immediately following infection from initial access, the victim's system would reach out to the malicious site and download the loader BOBC3953C59DA7870, spawning a rundll32.exe process. The loader would check if Telegram was installed and inject the primary payload into explorer.exe [47]. The group would use an information stealer file called

"*CO9D5A739B85C37C1*" to steal information from the Android device. The C2 communications were all done via the public SOAP API [47]. The XML-based data structure allowed communications between the victim and the attacker's C2 infrastructure.

G. Activity Cluster 7

a) Associated Activity Clusters: Pioneer Kitten, FoxKitten, PARISITE, UNC757

b) Overview: According to the security entity Crowdstrike, these activity clusters have been operating since 2017 and have a last known activity of 2020. This group's primary target has been gaining sensitive intelligence that would aid the Iranian government [48].

c) Initial Access: The threat groups have been known to utilize multiple CVE exploits to gain initial access into networks [49]. The most recent CVEs used by these activity clusters are CVE-2019-11510, CVE-2019-11539, CVE-2019-19781, and CVE-2020-5902, in which the group was able to leverage a vulnerability in VPN and network appliances to obtain a foothold in networks [49]. An interesting report has come from the Dragos Security organization that has claimed that Pioneer Kitten has worked as an initial access agent that propelled further operations for APT-33 (also known as Magnallium) [50].

d) Associated Malware: These threat clusters are not known for producing zero days and custom malware; instead, they opt for reworking public proof of concepts and CVEs for their malware [51]. CISA has found that the speed of their exploit creation has sped up, and the threat actor can produce "1-day" attacks much quicker after public notice and attempts to capitalize in the time period before organizations can patch their systems [50]. MITRE has also stated that the group leverages a variety of open-source tooling, including FRPC, Go Proxy, Nmap, Putty, PLink, TightVNC, and more [52].

H. Activity Cluster 8

a) Associated Activity Clusters: Static Kitten, Muddy Water, Seedworm

b) Overview: These activity clusters are known to conduct espionage campaigns and target multiple industries throughout the Middle East, Asia, Africa, Europe, and North America [13]. The groups were first observed in 2017 and have had speculated activity in November 2023. They have been attributed by the security firm Deep Instinct to be conducting a spear phishing campaign at the height of an ongoing conflict [53].

c) Initial Access: According to CISA, these activity clusters are known for conducting spear phishing campaigns with malicious .zip files with either an Excel document containing a malicious macro embedded or a malicious PDF document [54]. In one specific case, gaining initial access was conducted via compromised accounts in which legitimate documents were altered and embedded with malicious Microsoft Word macros and then sent to those expecting the document [55]. ClearSky Security identified the threat actors have shown a connection with the APT-42 group as they conducted the same exploit in 2019 as the APT-42 did in 2017. The attack consisted of two documents in which one displayed an "error" to a victim; one attachment would open the error message, while the second would immediately exploit a vulnerability after it was opened. This was a new TTP utilized by the activity cluster Muddy Water, and the virus signatures on their payloads were only identified by three antivirus engines, unlike their previous attacks in which 32 antivirus engines identified their payloads as malicious [56].

d) Associated Malware: The activity clusters were able to redevelop and modify an open-source project on GitHub called DNS_TXT_PWNAGE.ps1 to a malicious program called DNSMessenger that was dubbed POWERSOURCE by FireEye [54]. There was also attribution made by Unit 42 (Threat Intelligence Cell from Palo Alto) to a GitHub page used by the threat groups to stage and deliver payloads such as their POWERSTATS malware [50]. POWERSTATS is a PowerShell backdoor that communicates to a C2 infrastructure via RSA encryption and allows that threat group to maintain access in the network [54]. Clearsky Security identified the malware POWGOOP, which consists of five files that work in tandem to establish a DLL sideload to a signed Google Updater executable, which sets up a backdoor connection that can allow the group to run commands without raising suspicion [56].

I. Activity Cluster 9

a) Associated Activity Clusters: Cleaver, Threat Group 2889, TG-2889

b) Overview: These activity clusters have been attributed to Iran and were the primary attackers in "*Operation Cleaver*" and have been around since at least 2014 [57].

c) Initial Access: Cleaver has been identified using spear phishing and SQL Injection techniques for initial compromise onto their target networks. The spear phishing campaigns consisted of compromising victims with false job opportunities at an organization called Teledyne and using a copied resume website called easyresumecreator[.]com (legitimate website was winresume.com) [58].

d) Associated Malware: Cleaver used various modified open-source and custom malware, including Net Crawler, TinyZBot, zhcat, and zhmimikatz. Net Crawler is a tool developed in C# that would attempt to gather stored credentials from all computers on a network [58]. zhMimikatz and zhcat were open-source tools that were modified by Cleaver to remain more stealthy and conduct a few more functions. zhMimikatz was changed to allow the application to become completely automated, and zhcat was the open-source tool netcat, modified to allow for encrypted traffic, port mirroring, and other functions that its successor socat had already implemented [58]. TinyZBot was another C# custom backdoor tool that was used by Cleaver for two years and had become the longest-developed malware from this group [58]. TinyZBot utilized the SOAP API for its communications to and from the C2 infrastructure that was stood up by the threat group [58].

J. Activity Cluster 10

a) Associated Activity Clusters: Leafminer, RASPITE

b) Overview: These activity clusters have been attributed to have tremendous overlap and were first identified in 2017 according to MITRE [59]. Dragos, who identified RASPITE, found that the actor targeted electrical and industrial control systems (ICS) since mid-2017 [60].

c) Initial Access: The threat groups utilized multiple different avenues for initial access. The two activity clusters conducted watering hole attacks on compromised web servers, attempted to brute force login pages, and would openly scan publicly facing IP addresses for easy-to-exploit vulnerabilities before attacking them [59].

d) Associated Malware: Leafminer has taken advantage of two open-source projects on GitHub, including LaZagne and MailSniper. The threat actor used the Lazagne malware to conduct a post-exploitation enumeration of credentials stored on the victim machine [59]. MailSniper's primary goal is to systematically search through a mail server for specific strings and items of interest for an attacker. The tool also provided the activity clusters additional functionality such as password spraying, enumerating users, and dumping the Global Address List (GAL) for Outlook Web Access (OWA) exchange server [59]. These activity clusters also developed a custom RAT dubbed Sorgu that allows remote access to the victim machine. The group established persistence with this malware as it was installed as a service once executed [18]. Another malware used by Leafminer was their Trojan named Imecab, which allowed for persistent remote access to victim machines. This Trojan would create an account that could utilize remote access features and create a malicious executable named guester.exe that could be used as an indicator of compromise [18].

K. Activity Cluster 11

a) Associated Activity Clusters: CopyKittens

b) Overview: CopyKittens has been operating since 2013 and has become most famous for the "*Operation Tulip*" campaign in which the primary objective has been determined as foreign espionage on Israel, Saudi Arabia, Turkey, the United States, Jordan, and Germany [61].

c) Initial Access: CopyKittens primary initial access vector was phishing using a rich text file (.rtf) embedded with OLE objects and macros that would exploit the vulnerability associated with CVE-2017-0199 [62]. The phishing attachment was named IRAN_NORTH-KOREA_RUSSIA 20170420.docx and would reach out to a malicious C2 redirector at update.microsoft-office[.]solutions/license.doc and would then download the loader from aaa.stage.1404311.email.sharepoint-microsoft[.]com [62]. The CopyKittens APT also attempted initial access campaigns utilizing watering hole attacks and web-based exploitation [62].

d) Associated Malware: CopyKittens engaged in a campaign known as Wilted Tulip in which they introduced their custom malware MATRYOSHKA [61]. MATRYOSHKA was a custom dropper consisting of three parts: the dropper, reflective loader, and a RAT [61]. The dropper always had a consistent save location in the %TEMP% directory with a s̃t prefix, followed by seemingly random numbers and ending with a .pdf extension [61]. When the attack is conducted, the dropped reflective loader portion will load a library into a host process in the system's memory. This allows the RATs library to run without spawning a new process. This enables the RAT to remain a bit more stealthy, and finding the library is extremely difficult as it will not show under the loaded modules for the system. The RAT itself was signatured in 2015 as Trojan.Jectin by Symantec and Troj/Agent-AMEY by Sophos [61]. Another custom malware that CopyKittens created was TDTESS, a 64-bit .NET binary that initiates a reverse shell from the victim machine [62]. This malware creates a new service on the machine named bmwappushservice and deletes the log files of its installation once completed [62]. The threat actor performs good tradecraft as the file creation associated with the service creation becomes timestomped to the actual svchost.exe to blend in [62]. Timestomping is changing dropped file times and dates in the system to match another legitimate file. So the dropped file from the adversary has the same time and date of creation as svchost.exe in this case. This allows the malicious file to blend in more as the creation date is not brand new.

VI. Results and Findings

A. Common Initial Access Vectors

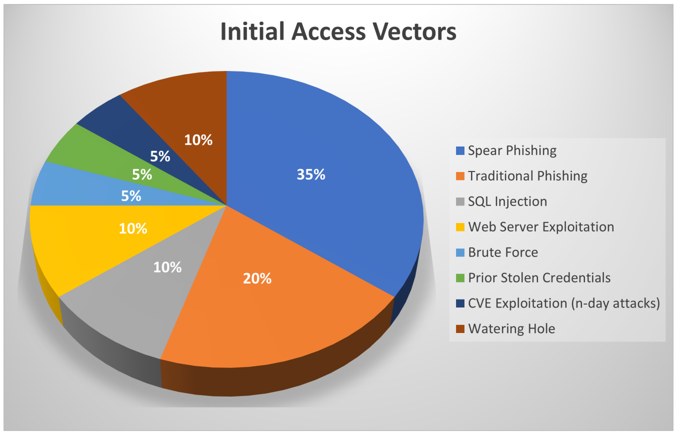

Fig. 3: Initial Access Vectors Across Iran APT Groups

The eleven Iranian-based activity clusters have used multiple vectors to gain initial access; however, there are two clear standout techniques being spear phishing and traditional phishing. Phishing is a social engineering attack that uses email or other messaging platforms to stage malware with malicious URLs, persuade the victim to give money, or elicit sensitive information from the victims. Phishing was a prominent initial access vector between the different clusters accounting for nine

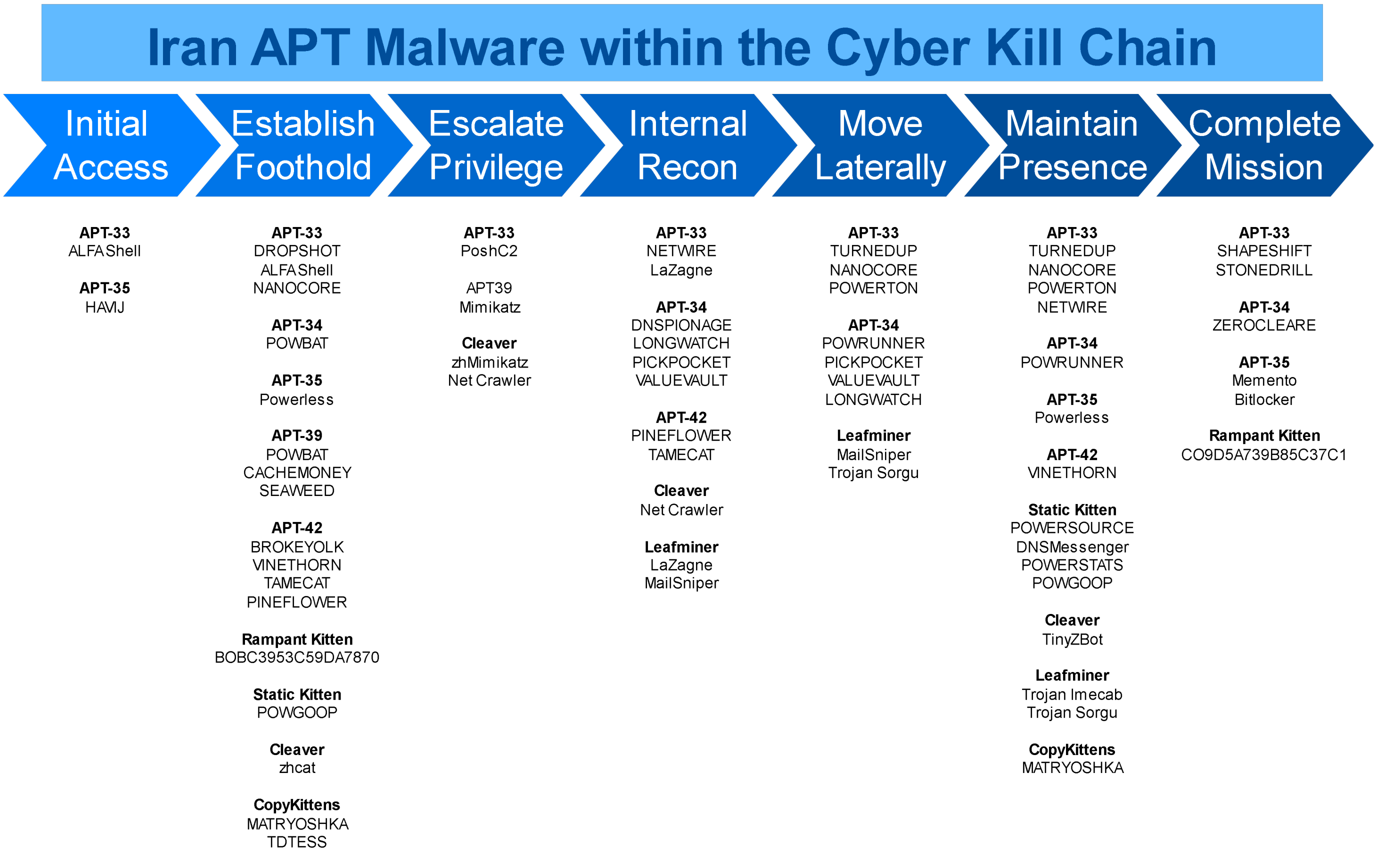

Fig. 4: Iran APT Malware Within the Cyber Kill Chain

of the eleven threat actors. Of the nine phishing initial access vectors, seven were spear phishing, and three used traditional phishing (1 activity cluster used both methods). Only counting the nine initial access vectors that used phishing methods, a common trend of using embedded macro documents arose. Seven of the nine groups used spear phishing as an initial access method. Phishing attempts featuring attachments with embedded macros are an attack vector the Iranian APT groups have found to be consistently exploitable. Figure 3 displays the initial access vectors found throughout the research. Phishing as a whole takes up 55% of the chart, with spear phishing taking 35% of the table and traditional phishing at 20%. The secondary avenues behind phishing methods were watering holes, SQL injection, and web server exploitation.

A trend discovered while looking at the phishing techniques of these activity clusters was the use of job-related lures against the victims. Of the nine groups that used phishing techniques, three clusters utilized job-related phishing campaigns to lure the victims into clicking malicious attachments.

B. Malware Similarities

One commonality between the malware was the use of the SOAP API to communicate to and from C2 infrastructure. APT-42, Rampant Kitten, and Cleaver used the SOAP API in their C2 communications with their malware to issue commands to their backdoors. The SOAP API can be used to secure communications and is a robust set of features that can be implemented to secure the connection. SOAP could be a common communication channel for these threat groups as the connections can be secured with WS-Security (Web Services Security), which allows for encryption, integrity, authentication, authorization, and timestamps [63]. SOAP is commonly used to secure web communications from servers utilizing HTTP; however, the API is also compatible with HTTPS which encrypts communications. Kuehnhausen and Frost [64] proposed a solution to capture SOAP messages as they traversed in and out of a network. There was an entire framework that was built around logging these types of communications and being able to analyze them [64]. If there is a continued pattern of threat actors utilizing this method of communication, implementing this framework could allow defenders to catch and monitor the SOAP messages on their networks and set triggers to alert on.

The researcher has mapped the activity clusters associated malware to the Cyber Kill Chain in Figure 4. This list is not exhaustive of all malware that the activity clusters have been associated with, as each cluster may have additional malware that goes by a different name that wasn't found in the research. The malware has been placed on the cyber kill chain based on the functionality of the malware itself and the primary objective it is attempting to accomplish. Some sections are smaller than others due to alternative methods that do not include malware utilized by the activity clusters, instead manual or scripted techniques (i.e., dumping hashes, phishing, service manipulations, service creation, registry changes, etc.).

Another common recurrence in the research was the use of .NET binaries by multiple activity clusters. It was found that the activity clusters dubbed APT-34, APT-35, APT-42, and CopyKittens all used different .NET binaries in their malware which could be a sign for the future. PowerShell has become a main focus in the defensive security world as it is used by many threat actors, and a gradual move to writing malware in C languages has been on the rise [65]. One major group to do this is SpecterOps with their "*GhostPack*" repository on GitHub [66]. Some of the tools that are included in this pack are direct ports of malware that have been re-written in C#. Some examples include SharpDump (PowerSploit's Out-Minidump.ps1), SharpUp (PowerUp.ps1), SharpDPAPI (some MimiKatz DPAPI functions) [66]. The defenses are not as good for malware written in C languages such as C# while also being able to be used on any version of .NET, making it more universal for exploiting most systems for the attackers [65]. This can be seen by security vendors porting over PowerShell malware to languages such as C#, C++, or C proper. Moving to these languages lets the attacker directly interface with the Windows function call APIs [67].

VII. Research Limitations

The primary limitation of this study is that it is based solely on open-source information and reports from various threat intelligence vendors, including Mandiant, Unit 42, Clearsky Cyber, Talos, and others. The study doesn't include classified data on APTs. As a result, the threat actors may utilize undisclosed Tactics, Techniques, and Procedures (TTPs) that reside at the proprietary or higher classification levels, thus they were not included in this research.

Another notable limitation lies in the attribution of threats to specific threat clusters. There might be additional threat cells and groups associated with Iran that have yet to be definitively attributed by intelligence agencies. Consequently, our research only focuses on activity clusters conclusively attributed to Iran. The malware attributed to the threat groups in this document has already been found and signatured by security entities. There is potentially other malware being used by these threat groups not mentioned in this research that has not been identified or found yet (i.e., zero days). Moreover, as technology and strategies evolve, the adversary's TTPs are subject to change, necessitating continuous updates and revisions to maintain the accuracy and relevance of the aggregated data and findings.

VIII. Future Work

Numerous areas of APT groups warrant deeper exploration, such as their TTPs, deep malware inspection, and network analysis. Conducting reverse engineering on the malware to discover which Windows Event Codes trigger when each malware is running and discovering if new processes and threads are being spawned with the Windows Process Monitor (procmon.exe) and much deeper technical research can be done. Throughout the research, these threat intelligence organizations found and presented indicators of compromise, which could greatly benefit the Cyber Threat Intelligence community with STIX and TAXII formatting. Delving into deep malware analysis and developing actionable machine-readable alerts for each piece of malware would be the next step in this research.

Social engineering awareness needs to be included in follow-up work, and a basis needs to be set for training individuals on the recognition of phishing attempts. Conducting experiments to discover which methods of training can lead to improvement in social engineering recognition. The human is the most significant liability to an organization's network, and the APT groups know and have been proven to take advantage of the vulnerability.

IX. Conclusion

In conclusion, the study reveals notable similarities in the initial attack techniques and malware used by Iranian APTs. Research on the topic has led to the discovery that Iranian APTs use spear and traditional phishing campaigns as their primary initial access vector beyond all other options. Phishing is a widespread trend among 9 of the 11 APT groups. Social engineering awareness campaigns should be implemented for all individuals to educate society on how to identify phishing and social engineering. It has been deemed trivial to know that the attackers use this method to compromise networks; however, there hasn't been a significant initiative to inform and educate the public. Training and awareness have been proven to lower the risk of social engineering attacks, but how do we get this training to everyone? Those who do not work in the cyber sector are at a higher risk of not getting the exposure and awareness training so many cyber professionals receive each year.

Similarities have been found in the activity clusters malware that can aid a network defender. .NET binaries were a common trend amongst some activity clusters. Activity clusters can directly make Windows function calls with C programming languages, bypassing some defenses that would get caught if run with PowerShell. Because of this, there have been many ports of PowerShell tools into C# programs. The defenders need to implement system call monitoring tools. SOAP API communications with threat actor C2 channels have also become common amongst some clusters. There are network monitoring tools and an entire framework mentioned that can allow a network defender to monitor the SOAP communications on their network.

In closing, Iranian activity groups are very dangerous and have been successful in many attacks; however, many more threat groups may be operating under the Iranian banner that has not been attributed yet. These unattributed threat actors could be exposed for working for Russia, Iran, China, or any other nation at any time. It is necessary to correctly identify threat actor patterns and TTPs when preparing defenses, making this research crucial. Discovering such operational trends underscores the importance of continuous research and vigilance to effectively anticipate and counter evolving threat landscapes. Furthermore, the study advocates for enhancing societal cybersecurity awareness, particularly regarding phishing and social engineering, as a pivotal component of a robust defensive posture against sophisticated APT threats.

REFERENCES

[1] “Advanced Persistent Threat (APT) Groups & Threat Actors,” Mandiant. Accessed: Oct. 30, 2023. [Online]. Available: https://www.mandiant.com/resources/insights/apt-groups

[2] P. Diotte, “The Big Four and Cyber Espionage: How China, Russia, Iran and North Korea Spy Online,” vol. 20, no. 4, 2020.

[3] Joint Task Force Transformation Initiative, “Managing information security risk:: organization, mission, and information system view,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-39, 2011. doi: 10.6028/NIST.SP.800-39

[4] K. Nickels, “Making Order out of Chaos: How to Deal with Threat Group Names — STAR Webcast.” Accessed: Nov. 16, 2023. [Online]. Available: https://www.youtube.com/watch?v=fV_9X9gnTIk

[5] ”Groups — MITRE ATT&CK®.” Accessed: Nov. 16, 2023. [Online]. Available: https://attack.mitre.org/groups/

[6] S. Caltagirone, A. Pendergast, and C. Betz, “The Diamond Model of Intrusion Analysis,” Jul. 2020.

[7] P. Chen, L. Desmet, and C. Huygens, “A Study on Advanced Persistent Threats,” in Advanced Information Systems Engineering, vol. 7908, C. Salinesi, M. C. Norrie, and Ó. Pastor, Eds., in Lecture Notes in Computer Science, vol. 7908. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 63–72. doi: 10.1007/978-3-662-44885-4_5. https://www.journal.forces.gc.ca/vol20/no4/PDF/CMJ204Ep32.pdf.

[8] “M-Trends 2022: Mandiant Special Report.” Mandiant, 2022. Accessed: Oct. 30, 2023. [Online]. Available: https://services.google.com/fh/files/misc/m-trends-report-2022-en.pdf

[9] “APT1: Exposing One of China’s Cyber Espionage Units.” Sep. 01, 2021. Accessed: Oct. 30, 2023. [Online]. Available: https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

[10] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, “A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1851–1877, 2019, doi: 10.1109/COMST.2019.2891891

[11] “Targeted Attack Lifecycle — Common Cyber Attack Lifecycles,” Mandiant. Accessed: Oct. 30, 2023. [Online]. Available: https://www.mandiant.com/resources/insights/targeted-attack-lifecycle

[12] “MITRE ATT&CK®.” Accessed: Oct. 30, 2023. [Online]. Available: https://attack.mitre.org/

[13] MITRE ATT&CK, “APT33, HOLMIUM, Elfin, Group G0064 — MITRE ATT&CK®.” Accessed: Nov. 12, 2023. [Online]. Available: https://attack.mitre.org/groups/G0064/

[14] M. T. Intelligence, “Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets,” Microsoft Security. Accessed: Nov. 12, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/

[15] Mandiant Threat Intelligence, “APT33 Targets Aerospace & Energy Sectors — Spear Phishing,” Mandiant. Accessed: Nov. 09, 2023. [Online]. Available: https://www.mandiant.com/resources/blog/apt33-insights-into-iranian-cyber-espionage

[16] S. Shample, “Iranian APTs: An overview,” Middle East Institute. Accessed: Oct. 30, 2023. [Online]. Available: https://www.mei.edu/publications/iranian-apts-overview

[17] J. O’Leary, “Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware.” Accessed: Nov. 09, 2023. [Online]. Available: https://tagteam.harvard.edu/hub_feeds/4280/feed_items/2841535

[18] J. G. Spataro, “Iranian Cyber Espionage,” M.S., Utica College, United States – New York. Accessed: Nov. 09, 2023. [Online]. Available: https://www.proquest.com/docview/2228240927/abstract/18D2FC7EF0F24300PQ/1

[19] Kaspersky Lab, “From SHAMOON to STONEDRILL: Wipers Attacking Saudi Organizations and Beyond.” Accessed: Nov. 12, 2023. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf

[20] M. K. Demirhan, “rat-collection.” Oct. 23, 2023. Accessed: Nov. 12, 2023. [Online]. Available: https://github.com/mstfknn/rat-collection/tree/master/4%20Nanocore%20Rat

[21] Nicolau, “alfa-shell.” Nov. 06, 2023. Accessed: Nov. 12, 2023. [Online]. Available: https://github.com/nicxlau/alfa-shell

[22] MITRE ATT&CK, “OilRig, COBALT GYPSY, IRN2, APT34, Helix Kitten, Evasive Serpens, Group G0049 — MITRE ATT&CK®,” MITRE ATT&CK. Accessed: Nov. 12, 2023. [Online]. Available: https://attack.mitre.org/groups/G0049/

[23] HivePro Labs, “Iranian-OilRig-Group-Strikes-with-AutoHotkey-Keylogger-and-Malicious-Macro_TA2023065.pdf.” Accessed: Nov. 12, 2023. [Online]. Available: https://www.hivepro.com/wp-content/uploads/2023/02/Iranian-OilRig-Group-Strikes-with-AutoHotkey-Keylogger-and-Malicious-Macro_TA2023065.pdf

[24] M. Fahmy, S. Magdy, and M. Zohdy, “New APT34 Malware Targets The Middle East,” Trend Micro. Accessed: Nov. 12, 2023. [Online]. Available: https://www.trendmicro.com/en_vn/research/23/b/new-apt34-malware-targets-the-middle-east.html

[25] Mandiant, “New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit,” Mandiant. Accessed: Nov. 12, 2023. [Online]. Available: https://www.mandiant.com/resources/blog/targeted-attack-in-middle-east-by-apt34

[26] S. Hawley, B. Read, C. Brafman-Kittner, N. Fraser, Y. Rozhansky, and S. Yashar, “APT39: An Iranian Cyber Espionage Group Focused on Personal Information,” Jan. 2019.

[27] K. Berglyd, “Strategic Culture and State Behaviour in Cyberspace.” Accessed: Nov. 08, 2023. [Online]. Available: https://www.duo.uio.no/bitstream/handle/10852/96599/STV4992-Master-s-Thesis-Knut-Joachim-Tander–Berglyd-Spring-2022.pdf?sequence=1&isAllowed=y

[28] Michaelab, “Iran’s APT34 Returns with an Updated Arsenal,” Check Point Research. Accessed: Nov. 09, 2023. [Online]. Available: https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/

[29] W. Mercer and P. Rascagneres, “DNSpionage Campaign Targets Middle East,” Cisco Talos Blog. Accessed: Nov. 09, 2023. [Online]. Available: https://blog.talosintelligence.com/dnspionage-campaign-targets-middle-east/

[30] M. Bromiley, N. Klapprodt, N. Schroeder, and J. Rocchio, “Hard Pass: Declining APT34’s Invite to Join Their Professional Network,” Mandiant. Accessed: Nov. 12, 2023. [Online]. Available: https://www.mandiant.com/resources/blog/hard-pass-declining-apt34-invite-to-join-their-professional-network

[31] M. T. Intelligence, “Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets,” Microsoft Security Blog. Accessed: Nov. 16, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/

[32] “Magic Hound, TA453, COBALT ILLUSION, Charming Kitten, ITG18, Phosphorus, Newscaster, APT35, Group G0059 — MITRE ATT&CK®.” Accessed: Nov. 16, 2023. [Online]. Available: https://attack.mitre.org/groups/G0059/

[33] ClearSky Security, “The-Kittens-Are-Back-in-Town-2.pdf.” Accessed: Nov. 10, 2023. [Online]. Available: https://www.clearskysec.com/wp-content/uploads/2019/10/The-Kittens-Are-Back-in-Town-2.pdf

[34] M. T. Intelligence, “Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021,” Microsoft Security Blog. Accessed: Nov. 12, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/

[35] Avertium, “An In-Depth Look at APT35 aka Charming Kitten,” Avertium. Accessed: Nov. 09, 2023. [Online]. Available: https://explore.avertium.com/resource/in-depth-look-at-apt35-aka-charming-kitten

[36] D. Frank, “PowerLess Trojan: Iranian APT Phosphorus Adds New PowerShell Backdoor for Espionage.” Accessed: Nov. 12, 2023. [Online]. Available: https://www.cybereason.com/blog/research/powerless-trojan-iranian-apt-phosphorus-adds-new-powershell-backdoor-for-espionage

[37] MITRE ATT&CK, “Havij, Software S0224 — MITRE ATT&CK®.” Accessed: Nov. 12, 2023. [Online]. Available: https://attack.mitre.org/software/S0224/

[38] M. T. Intelligence, “Profiling DEV-0270: PHOSPHORUS’ ransomware operations,” Microsoft Security Blog. Accessed: Nov. 12, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2022/09/07/profiling-dev-0270-phosphorus-ransomware-operations/

[39] S. Hawley, B. Read, C. Brafman-Kittner, A. Thompson, Y. Rozhansky, and S. Yashar, “APT39 — Iranian Threat Group Focused on Personal Information,” Mandiant. Accessed: Nov. 10, 2023. [Online]. Available: https://www.mandiant.com/resources/blog/apt39-iranian-cyber-espionage-group-focused-on-personal-information

[40] “APT39, ITG07, Chafer, Remix Kitten, Group G0087 — MITRE ATT&CK®.” Accessed: Nov. 16, 2023. [Online]. Available: https://attack.mitre.org/groups/G0087/

[41] “CISA Analysis - FY2020 Risk and Vulnerability Assessments,” Jul. 2021, Accessed: Nov. 12, 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/FY20-RVA-Analysis_508C.pdf

[42] Mandiant, “APT42: Crooked Charms, Cons and Compromises.” Accessed: Nov. 16, 2023. [Online]. Available: https://services.google.com/fh/files/misc/apt42-crooked-charms-cons-and-compromises.pdf

[43] S. Ozeren, “Emerging Cyber Threats of September 2022,” Picus Security. Accessed: Nov. 12, 2023. [Online]. Available: https://www.picussecurity.com/resource/blog/emerging-cyber-threats-of-september-2022

[44] C. Labs, “Iran’s Cyber Espionage Operations: The Case of the APT42 Threat Group — Cyware — Research and Analysis,” Cyware Labs. Accessed: Nov. 12, 2023. [Online]. Available: https://cyware.com/resources/research-and-analysis/irans-cyber-espionage-operations-the-case-of-the-apt42-threat-group-1e6d

[45] E. Haeghebaert, “VB2021-Haeghebaert.pdf.” Accessed: Nov. 10, 2023. [Online]. Available: https://vblocalhost.com/uploads/VB2021-Haeghebaert.pdf

[46] “Dark Web Profile: APT42 - Iranian Cyber Espionage Group - SOCRadar,” SOCRadar® Cyber Intelligence Inc. Accessed: Nov. 12, 2023. [Online]. Available: https://socradar.io/dark-web-profile-apt42-iranian-cyber-espionage-group/

[47] Lotemf, “Rampant kitten - an Iranian espionage campaign,” Check Point Research, https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/#infection_chain (accessed Nov. 13, 2023).

[48] A. Orleans, “PIONEER KITTEN: Targets & Methods [Adversary Profile],” crowdstrike.com. Accessed: Nov. 16, 2023. [Online]. Available: https://www.crowdstrike.com/blog/who-is-pioneer-kitten/

[49] “Iran-Based Threat Actor Exploits VPN Vulnerabilities — CISA.” Accessed: Nov. 13, 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-259a

[50] “North American Electric Cyber Threat Perspective,” 2020, [Online]. Available: https://www.dragos.com/wp-content/uploads/NA-EL-Threat-Perspective-2019.pdf

[51] A. Fixler and T. Logan, “Pioneer Kitten: A New Iranian Cyber Threat Group Emerges,” FDD. Accessed: Nov. 13, 2023. [Online]. Available: https://www.fdd.org/analysis/2020/09/16/pioneer-kitten-new-iranian-cyber-threat/

[52] “Fox Kitten, UNC757, Parisite, Pioneer Kitten, Group G0117 — MITRE ATT&CK®.” Accessed: Nov. 13, 2023. [Online]. Available: https://attack.mitre.org/groups/G0117/

[53] S. Kenin, “MuddyWater eN-Able spear-phishing with new TTPs — Deep Instinct Blog,” Deep Instinct. Accessed: Nov. 16, 2023. [Online]. Available: https://www.deepinstinct.com/blog/muddywater-en-able-spear-phishing-with-new-ttps

[54] “Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks — CISA.” Accessed: Nov. 13, 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-055a

[55] [1] T. Lancaster, “Muddying the Water: Targeted Attacks in the Middle East,” Unit 42. Accessed: Nov. 10, 2023. [Online]. Available: https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

[56] “Iranian APT group ‘MuddyWater’ Adds Exploits to Their Arsenal.” Accessed: Nov. 10, 2023. [Online]. Available: https://www.clearskysec.com/wp-content/uploads/2019/06/Clearsky-Iranian-APT-group-%E2%80%98MuddyWater%E2%80%99-Adds-Exploits-to-Their-Arsenal.pdf

[57] “Cleaver, Threat Group 2889, TG-2889, Group G0003 — MITRE ATT&CK®.” Accessed: Nov. 16, 2023. [Online]. Available: https://attack.mitre.org/groups/G0003/

[58] “Cylance-Operation-Cleaver-Report-1748-1833.pdf.” Accessed: Nov. 13, 2023. [Online]. Available: https://www.aclu.org/wp-content/uploads/legal-documents/Cylance-Operation-Cleaver-Report-1748-1833.pdf

[59] “Leafminer, Raspite, Group G0077 — MITRE ATT&CK®.” Accessed: Nov. 13, 2023. [Online]. Available: https://attack.mitre.org/groups/G0077/

[60] “Threat Group RASPITE — Dragos.” Accessed: Nov. 16, 2023. [Online]. Available: https://www.dragos.com/threat/raspite/

[61] ClearSky Security and Trend Micro, “Operation_Wilted_Tulip.pdf.” Accessed: Nov. 09, 2023. [Online]. Available: https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf

[62] Minerva Labs and ClearSky Cyber Security, “CopyKittens Attack Group.” Accessed: Nov. 13, 2023. [Online]. Available: https://cyberwarzone.com/wp-content/uploads/papers/Minerva_Clearsky_CopyKittens(11-23-15).pdf

[63] R. Kumar, K. Rajaram, and C. Babu, Security for SOAP based Communication among Web Services. 2013.

[64] M. Kuehnhausen and V. Frost, “Framework for Analyzing SOAP Messages in Web Service Environments.” Accessed: Nov. 14, 2023. [Online]. Available: http://www.rsl.ku.edu/publications/documents/Kuehnhausen2010_TR-41420-20.pdf

[65] C. B. Tom Stewart, “Penetration testers tool kit: A transition from PowerShell to C#,” Technology Insights Blog, 19-Oct-2020. [Online]. Available: https://tcblog.protiviti.com/2020/10/19/penetration-testers-tool-kit-a-transition-from-powershell-to-c/. [Accessed: 18-Nov-2023].

[66] “GhostPack,” GitHub. Accessed: Nov. 18, 2023. [Online]. Available: https://github.com/GhostPack

[67] “Bypassing user-mode hooks and direct invocation of system calls for Red Teams,” MDSec, 31-Dec-2020. [Online]. Available: https://www.mdsec.co.uk/2020/12/bypassing-user-mode-hooks-and-direct-invocation-of-system-calls-for-red-teams/. [Accessed: 18-Nov-2023].