IRANIAN CYBER ESPIONAGE

by

Jason G. Spataro

A Capstone Project Submitted to the Faculty of

Utica College

May 2019

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Cybersecurity

Abstract

The culture, history and language of Persia are indelible. Since the rule of Cyrus the Great in 550 BC, dynastic and monarchical Persian empires maintained hegemonic influence over the Middle East for 2500 years. This longstanding dominance dissipated in 1979, when a revolution was waged by multiple political factions against the last Shah of Iran, eventually leading to the usurp of power by a clergy-led state. From that point, the Islamic Republic of Iran has sought to reconstitute itself as a regional hegemony, expanding its presence by quietly inserting itself into surrounding conflicts. In the era of digital industrialization, where geographic boundaries are blurred by binary code, Iran leverages the cyberspace domain to conduct soft war against its adversaries, engaging in both destructive cyber operations and espionage-oriented ones. In an effort to provide a more detailed analysis on the latter of these two categories, IRANIAN CYBER ESPIONAGE outlines this use of cyber warfare to achieve intelligence objectives, chronicling and detailing tactics by the most prominent Iranian cyber threat actors, and analyzing the results to make determinations about Iran as a 21st century cyber power. Keywords, Utica College, Dr. Chris Riddell, Iran, cybersecurity, cyber espionage, cyber warfare.

Table of Contents

List of Illustrative Materials

Iranian Cyber Espionage

Cyber warfare is the new norm between nation-states exercising the benefits of "Soft War." The Islamic Republic of Iran is a rapidly developing contender within this quiet conflict. The purpose of this research is to study the capabilities of the cyber espionage operations undertaken by Iranian cyber threat actors. What the methodology is behind Iranian cyberattacks? What do the practices of Iranian cyber threat actors tell us about their strategy, structure, and purpose? What is the correlation between the Tactics, Techniques and Procedures (TTPs) utilized by Iranian cyber threat actors and those employed by Iran-linked groups outside the country?

In the executive summary of a threat intelligence report released in 2014, analysts at Cylance made a bold statement: "Iran is the new China." The report went on to detail an extensive cyber espionage campaign operating from Tehran, with targets ranging across sixteen countries, and whose array of TTPs were successful in establishing persistence in and harvesting sensitive data from key government and commercial institutions. It was not the first cyber espionage campaign from Iran, nor would it be the last.

Commentary on the Islamic Republic of Iran has traditionally revolved around its nuclear program, as well as to its longstanding partnerships with and support of insurgent and terrorist groups across the Middle East (Morell & Harlow, 2015). However, in the age of digital industrialization, Iran has demonstrated significant capabilities as a threat actor within cyberspace, with a growing multitude of successful, large-scale attacks against a wide variety of systems and targets.

Understanding the methodology of Iranian cyberattacks is an exercise in mapping out every major avenue of attack that cyber threat actors associated with the country have exhibited

the ability to carry out. As Iran continues to practice cyber warfare as a means of statecraft, it becomes increasingly important to recognize what cyberattack methods it is capable of conducting. Doing so will provide a defined scope with which to view its role in the international arena of cyberspace. It will also help bridge a knowledge gap resulting from the expedited pace at which Iran's cyber capabilities have developed. FireEye (2018) underscored this knowledge gap in its report on annual cybersecurity trends, stating that Iran's notoriety for destructive cyberattacks has overshadowed its vast cyber espionage campaigns, the likes of which "currently spans nearly every industry sector and extends well beyond regional conflicts in the Middle East." FireEye goes on to recognize that Iranian TTPs had advanced yet again, this time in such a way that enables attackers to hold a simultaneous presence within multiple targets for months and even years at a time. Furthermore, they highlight that TTPs now consist of custom-built malware constructed by Iranian cyber threat actors to function precisely against specific targets.

In the same FireEye (2018) report, analysts established an important connection between cyber espionage and destructive cyberattacks, the two overarching categories of Iranian cyber warfare. Exemplifying activities by the Advanced Persistent Threat (APT) labeled APT35, the authors detailed how attackers successfully authenticated and gained access to hundreds of cloud-based email boxes of an unnamed energy sector company, which were then leveraged to extract information about Middle Eastern partner organizations. On its own, this incident would have been considered cyber espionage. But the Middle Eastern organizations whose data was harvested from the compromised mailboxes were the subsequent targets of destructive cyberattacks, linking the two strategic archetypes into a more singular, complex cyber threat apparatus. A public blog entry by FireEye from the previous year contained a separate instance of this correlation. In it, authors recognized that APT33, known as a cyber espionage threat actor,

utilized information gathering malware for its core operations that was subtly provisioned with SHAPESHIFT, a destructive wiper used to completely clear data off hard drives. (O'Leary, Kimble, Vanderlee & Fraser, 2017). The SHAPESHIFT malware had not been actively deployed in the dropper module of APT33's cyberattacks, however, the attack methodology of Iranian threat actors in cyberspace had transitioned from cyber espionage into a destructive operation.

Collectively, the use of cyber espionage has been essential to Iran's cyberspace-based "soft war" strategy, and persists as a central element of Iranian statecraft. Therefore, research into their attack methodology is foundational in understanding the progression that Iran has made, the position it currently occupies, and the potential advancements it may subsequently seek to achieve.

By examining the TTPs of Iranian cyber threat actors alongside those of the militant groups and nation-states allied with the Iranian government, it may be possible to correlate patterns between known threat actors. If discovered, these patterns may denote mutual cooperation between Iran and its regional allies in the cyberspace domain.

The significance of these partnerships lies in the extensive history between the Islamic Republic of Iran and a conglomerate of distinct militant groups throughout the Middle East whose political interests align with those of the Iranian government. This web of regional partnerships culminated in the early 1980s, with the organization and sponsorship of Lebanese Hezbollah by the Iranian Revolutionary Guard Corps (IRGC), and continues in their support of militant groups today, such as Hamas, Palestinian Islamic Jihad, the Iraqi Special Groups (SGs), and the Houthi Movement (Levitt, 2015). With the sole nation-state addition of Syria, this nexus forms the whole of Iran's hard allies across the Middle Eastern region. Identities of these militant organizations are largely the same: each is a politically-motivated insurgency that thematically

applies Islamic identity in support of their cause. The Syrian government, Lebanese Hezbollah, and Hamas also occupy key political roles within their respective countries and territories (Nasr, 2006).

Within the digital realm, many of these same political and militant organizations have begun to conduct cyber espionage operations of their own, some of which have been noted by cybersecurity professionals as relatively sophisticated. Thus, it remains to be seen whether Iran supports these regional allies in cyberspace the same way it does politically and militarily. If so, it would underscore the potential for a future in which Iran's cyber warfare capabilities are wielded by multiple threat actors, several of whom have established histories waging irregular warfare against common adversaries, most notably Israel, the Kingdom of Saudi Arabia (KSA), and the United States (U.S.).

The proliferation of cyber warfare capabilities presents a serious threat to U.S. national security. Far beyond the logical impact of traditional cyberattacks, Iranian disruptive and destructive operations targeting critical national infrastructure have successfully breached the security systems of major telecommunications and transportation networks, including airlines and airports (Cylance, 2014). Another infiltration attempt targeted a dam in upstate New York (Eisenstadt, 2016). In the hands of a threat actor intent on causing immediate and grave harm to a civilian populace, these attacks could be used to damage ecosystems, sever communication networks, and infiltrate public transportation facilities. In addition, the opacity of cyber warfare means that attacks may be difficult to attribute to a particular party, and could bypass existing security measures put in place to thwart physical attacks.

The proliferation of cyber espionage capabilities would play a more niche role in supporting operations by insurgent and terrorist groups. Similar to how FireEye (2018) described

the capability of Iranian actors to conduct disruptive and destructive cyberattacks utilizing intelligence gathered through successful cyber espionage operations, so too could threat actors such as Lebanese Hezbollah leverage cyber espionage to gather intelligence against its adversaries, which it could then use in the context of physical attacks. Furthermore, these groups frequently either wage or participate in armed conflicts, such as the Syrian Civil War and the Yemen Civil War, and may benefit from strategic intelligence provided by cyber espionage. Cybersecurity firm Clearsky noted the increase in cyberattacks against Israeli infrastructure during the course of the 2014 Israeli-Gaza conflict (Gholee, 2014), which could suggest that cyber espionage operations have already served such a purpose.

Iran's deployment of cyber espionage allows it to gather intelligence against foreign entities in a new strategic and tactical capacity. This new capability allows access to targets hitherto inaccessible. Meanwhile, it does this while maintaining a means to circumvent direct responsibility, and, perhaps most importantly, to overcome the disparity between deficiencies of its own military and the strength and numerosity of its adversaries.

On the Structure of Iranian Cyber Espionage

The research conducted within the following literature review largely concerns the use of different TTPs by Iranian cyber threat actors within the course of their cyber espionage operations, and does not frequently discuss the larger Iranian cyber nexus, nor the cyber ecosystem internal to Iran. These subjects deviate from the chronology, capability, and strategy of Iranian cyber espionage that is the focus of the paper, and instead touch upon the much more obscure question of structure. Though not the underlying focus of the research conducted, this secondary subject is nonetheless contextually relevant, and serves as an underlying foundation to

the timeline of Iranian cyber threat actors and their operations. Therefore, this section will serve as a short background into the structure of Iran's cyber nexus.

A clear understanding of Iran's cyber nexus is difficult to achieve due to the highly dynamic nature of Iranian cyber threat actors within the country. These threat actors include sophisticated APTs, but also feature less prominent groups as well as individual attackers, all ranging in motive, scope, and competency. This scenario is further complicated by the rate at which threat actors appear and reappear, similarities between the TTPs of certain cyberattacks, and the use of shared resources between parties. All of this has led to a very murky interpretation of the Iranian cyber nexus, and it is sometimes unclear if a threat actor is operating from within the Iranian government, working on behalf of them, or is an independent hacktivist organization without direct affiliation to any overarching political powers. This paper does not produce an exhaustive list of Iranian cyber threat actors, and instead focuses on only the most prominent groups, but there is a much more extensive community of attackers that exist within Iran.

This community is briefly overviewed in a Recorded Future report by Gundert, Chohan and Lesnewich (2018) in their report on the hierarchy behind Iranian cyber operations. In it, the authors underscored that Iran's cyber ecosystem is led by the IRGC, and from there descends into a network of ideologically affiliated intelligence officials that connect the IRGC's tasks and priorities to bidding contractor organizations, which may compete against one another or work in tandem. Many of these contractors, such as Kavosh Security, ITSecTeam (ITSEC) and Mersad Company, are publicly documented, but the proliferation of Iranian cyber warfare and the aforementioned lifecycles of Iranian cyber threat actors make it difficult to determine exact how many contractors exist, who their members are, or what other roles they occupy within Iranian society.

Anderson and Sadjadpour (2018) claimed that the Iranian Ministry of Intelligence was also involved in offense cyber operations.

Below this tiered structure of government organizations and contractors, a subculture of cybersecurity amateurs and professionals congregate in forums such as Ashiyane, Simorgh and Delta Security. It is unclear exactly what the connection is between membership to these forums and the overarching contracting platform described above, but Gundert, Chohan and Lesnewich (2018) have made correlations between forum administrators and IRGC members. The authors describe the forums as "trust communities," in which Iranian contractors can leverage as a recruitment platform. Posts on these forums discuss trending TTPs, cyberattack strategies, the political ideology behind various cyberattacks, and targeting, and also serve as a medium within which individual attackers can boast their success to one another.

In their report, Gundert, Chohan and Lesnewich (2018) underscored the relationship between the Imam Hossein Comprehensive University (IHU) and Iran's cyber nexus, noting that IHU is strongly affiliated with the IRGC, the Iranian Ministry of Science, Research and Technology, and the Iranian Ministry of Defense and Armed Forces Logistics. Fixler and Cilluffo (2018) noted in their own report that the U.S. Treasury Department enacted sanctions against IHU in 2012 for its strong relationship and support of the IRGC and its operations. The IRGC itself was designated a terrorist group by the U.S. government in April 2019. Other universities, including Sharif University of Technology in Tehran, are believed to be tied to the cyber nexus, and the Iranian government is said to partner with these academic institutions to develop students with cybersecurity skillsets, where they can then be recruited by Iranian companies, contractors, and government organizations.

Note that, while the information presented here explains many obscurities surrounding the structure of Iranian cyber espionage, it is not absolute. The Recorded Future report by Gundert, Chohan and Lesnewich (2018), which serves as much of the basis for this background, was largely supported by unpublished interviews conducted between Recorded Future's Insikt Group and an anonymous Iranian, who is alleged to have direct insight into the cyber nexus due to his role in founding an Iranian cybersecurity forum. While this does not disqualify the findings of the report, it does leave open the possibility that not all details presented in it are factual or complete.

Literature Review

Numerous vendors, threat intelligence groups, and individual researchers have assigned different names to each cyber threat actor throughout its history. This has occasionally led to threat actors being studied based on singular cyberattacks or operations, and only later being connected to wider contexts as a previously identified threat actor. It has also caused threat actors to be referred to by a plethora of different aliases. The following research will cite each threat actor by one name only, and list the other names associated with its activities in its introduction. The referenced names for threat actors within this paper are based on the nomenclature of FireEye (2019), who congregate multiple Finished Intelligence (FIN) incidents into Temporary (TEMP) profiles, which, after considerable amounts of activity, are formally declared APTs and assigned a number. Exceptions will be made in the cases of Operation Cleaver and Leafminer, which have not been categorized within FireEye's public reports.

Iranian Cyber Espionage Campaign

APT33. APT33 is a cyber espionage threat actor whose operations target the military and commercial aviation industries of the U.S. and the KSA, as well as the petrochemical sectors of

the KSA and South Korea. Operating since at least 2013, APT33 has been noted for its recorded capabilities to engage in destructive cyberattacks, utilizing dormant TTPs that cybersecurity professionals have observed within the context of cyber espionage campaigns. In this way, APT33 is distinct from many other Iranian cyber threat actors in that the range of its operations is curtailed to a small subset of industries and nations. Analysts at FireEye have published that this makes the motives of the group more discernable, and that cyberattacks by APT33 indicate a desire to collect intelligence on the military aviation capabilities of the KSA, as well as a form of industrial espionage against South Korean petrochemical companies that have engaged in business both with the KSA and Iran (O'Leary, et al., 2017).

APT33 is purported to be tied to the Nasr Institute, a supposed offshoot of an organization known as the Iranian Cyber Army, both cyber threat actors affiliated with the Iranian government. APT33 is also believed to be connected to Operation Ababil, a series of cyberattacks against financial institutions occurring between 2011 and 2013 (O'Leary, et al., 2017). However, these correlations are not definite, and the numerous similarities and potential links are representative of the obscurity with which Iranian cyber threat actors operate.

Authors of FireEye's report have recorded that a spear phishing campaign targeted workers in the aviation industry, using emails posed as recruitment opportunities to leverage malicious Hypertext Markup Language (HTML) application (.hta) files. The .hta files contained embedded code that would download a custom-made ALFASHELL backdoor. ALFASHELL is a prominent spear phishing toolkit within the Iranian hacking community. APT33 has been observed making errors in its use of the tool, for example, it has accidentally sent out spear phishing attacks with default values left in the content of the emails, only to resend those attacks shortly thereafter (O'Leary, et al., 2017).

This spear phishing campaign was bulwarked by the use of domain masquerading techniques that attackers employed to better resemble legitimate companies within the industry that they targeted. For instance, domains used in cyberattacks against the aviation sector had been registered to mirror Boeing, Northrop Grumman Aviation Arabia (NGAAKSA), Alsalam Aircraft Company and Vinell Arabia (O'Leary, et al., 2017).

APT33's cyber arsenal includes several different backdoors used for maintaining presence, the majority of which are connected to custom-made malware known to circulate within Iranian hacker communities, and others which are publicly available outside of Iran. These include NANOCORE, NETWIRE, TWINSERVE, TURNEDUP and DROPBACK. The group has also been observed using the open-source Mimikatz and ProcDump to escalate privileges, internal Windows functions such as PsExec Windows Management Instrumentation (WMI) to pivot between systems within the target network, and the open-source PowerSploit framework to conduct internal reconnaissance. Data exfiltration has been performed using the WinRAR tool for file compression, hidden directories to mask the data, and file uploading software to communicate with command-and-control (C2) infrastructure (O'Leary, et al., 2017). C2 infrastructure are servers that an attacker can leverage throughout the course of a cyberattack to store malware, forward stolen data, and maintain communication with a compromised host.

APT34. APT34, also referred to as OilRig and Helix Kitten, is an Iranian cyber espionage APT whose cyber warfare operations extend back to at least 2014. They have predominantly waged cyberattacks within the Middle East region, with frequent targets in the financial, energy, and government sectors (FireEye, 2018). At one point in time, cybersecurity vendors tracked two separate Iranian cyber threat actors coined Cadelle and Chafer, but further research indicated that these two threat actors were likely both APT34, or directly connected to it

("Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford", 2018).

Singh and Chang (2016) first reported that a threat actor, later identified as APT34, had sent weaponized Microsoft Excel documents with malicious macros to employees across the Middle Eastern banking industry. Emails delivering these weaponized documents took the guise of information technology (IT) log reports. Malicious macros obfuscated content with base64-encodeding, created new directories on the target computer, and then created a scheduled task masked as a Google service, which quietly ran a Visual Basic Studio (VBS) script in the background of the computer every three minutes. Authors noted that after the malicious macros had been enabled on the weaponized document, users would see additional content appear within the document. This added a new layer of social engineering to the context of the attack: by displaying additional content, the attackers better made the weaponized document function as a regular one would be expected to, thus reducing the likelihood that the cyberattack would invoke suspicion on part of the user.

The VBS script running in the background of the computer would download content from the attackers' C2 infrastructure, which included a customized version of the Mimikatz penetration testing toolkit. In addition, a malicious batch (.bat) file was fetched from the respective infrastructure and used to gather system information, including the current user, network configuration data, other user and group accounts, administrator accounts, and running processes (Singh & Chang, 2016).

Finally, data exfiltration would be performed through the use of DNS queries, which authors underscored was used for standard operations and was unlikely to be blocked or raise the suspicion of cybersecurity professionals. A separate PowerShell script was used to communicate

with C2 servers. The PowerShell script would communicate with the C2 servers by making a series of DNS queries, and used each octet of the Internet Protocol (IP) addresses listed within the DNS queries as code to transmit the targeted data. In this scenario, the octets of numbers within the IP addresses were converted from decimal representation into hexadecimal representation, which signified American Standard Code for Information Interchange (ASCII) characters that would then spell out the contents of the exfiltrated data. The C2 servers would conclude this data stream by replying to the DNS queries with an IP address of 35.35.35.35, at which point relevant files would be uploaded to the C2 DNS server, and remnants of the operation would be deleted from the computer until the PowerShell script was again called upon (Singh & Chang, 2016).

Palo Alto Networks covered APT34 extensively between 2016 and 2018, first writing in their Unit 42 cybersecurity blog that the APT had primarily targeted financial institutions within the KSA. They referred to the same VBS script and PowerShell script, which they named the Helminth backdoor (Falcone & Lee, 2016). This initial report largely aligned with the aforementioned findings by FireEye, who had not yet recognized the APT in an official capacity.

Later, Grunzweig and Falcone (2016) wrote for Palo Alto Networks' Unit 42 cybersecurity blog that APT34 had updated its TTPs and broadened its range of targets, bringing weaponized Microsoft Excel documents embedded with malicious macros to Turkish government entities and Qatari organizations. In addition, the original VBS script used in their cyberattacks had been expanded, and three other VBS scripts were now also employed, each with their own corresponding PowerShell script. The scripts possessed only minor differences, mostly relegated to the domain name and IP address used for respective C2 infrastructure. Authors underscored that APT34 had been able to penetrate major institutions without highly

sophisticated attacks, instead leveraging more straight forward techniques that were exceptionally difficult to detect.

ClearSky published to their cybersecurity blog that APT34 had targeted an undisclosed number of Israeli organizations since late 2015, and that their spear phishing campaigns had leveraged the compromised accounts of initial targets to work their way towards secondary, more valuable targets. Their distributed malware was also digitally signed with a valid signing certificate issued by Symantec to AI Squared. AI Squared later confirmed that this digital certificate had been compromised and would be revoked (“Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford", 2017).

Authors at FireEye published in their Threat Research blog that APT34 had exploited CVE-2017-11882 less than a week after Microsoft had publicly released a patch for it. CVE-2017-11882 was a memory-based vulnerability that allowed remote arbitrary code execution, and functioned in such a way that the code would appear to have been run by the current user. APT34 continued to use weaponized documents to establish initial compromise, but instead of malicious macros, the Rich Text Format (.rtf) documents used would exploit the CVE-2017-11882 memory vulnerability, downloading additional malicious scripts through the creation of child processes, and establishing communications with C2 infrastructure. At this point, the aforementioned VBS script and two updated PowerShell scripts would execute on the target system every minute. The first of these PowerShell scripts was a PowerShell backdoor named POWRUNER was used to send and receive commands from the C2 infrastructure, and would execute every minute. POWRUNER functioned by receiving a random 11-digit number from the C2 server, and interpreting the final digit of this number as a command associated with a particular action. POWRUNER was also capable of receiving batch commands from C2

infrastructure, instructing it to collect information from the compromised system. The second PowerShell script, BONDUPDATER, utilized Domain Generation Algorithms (DGA) to generate subdomains from within which it could communicate with C2 servers (Sardiwal, Cannon, Londhe, Richard, & O'Leary, 2017).

Lee and Falcone (2018) later published APT34's expanded their TTPs, delivering Trojan malware and new weaponized Microsoft Office documents via spear phishing campaigns. The advancements made by these new methods of compromise further obscured communication between malware and the C2 infrastructure. Several months later, Lee and Falcone (2018) confirmed that their findings on APT34 had aligned with those previously made by FireEye and ClearSky. They also highlighted that APT34 had again expanded their TTPs, now utilizing malicious executable files compiled in the Microsoft .NET Framework to establish initial compromise. After the malicious executable had run, a decoy dialog box was deployed on the user's screen to reduce suspicion, and the PowerShell-based QUADAGENT backdoor was installed onto the user's computer. QUADAGENT would then go on to communicate with C2 infrastructure and conduct data exfiltration. The open-source tool Invoke-Obfuscation was used in conjunction with QUADAGENT for obscurity, changing the variables and the strings of the QUADAGENT script in order to facilitate its installation and mitigate its detection.

In April 2019, a Telegram channel titled Lab Dookhtegan, a Farsi-language term referencing people whose lips have been sewn shut, was created by an anonymous user or group of users who claimed to have compromised servers belonging to the Iranian Ministry of Intelligence. Lab Dookhtegan referenced the Iranian Ministry of Intelligence and APT34 as one in the same. Messages by the Telegram channel were written in both Farsi and English, although the Farsi content resembled the language of a native speaker, while the English content did not.

The initial messages by Lab Dookhtegan declared opposition to the Iranian Ministry of Intelligence, and stated an intent to release information about APT34, including the identities of its leaders, the goals of its cyberattacks, and specific tools that it uses. Following messages contained .zip files of APT34 malware dubbed POISONFROG and another named GLIMPSE (see Figure 1), the former an older and latter a newer version of the BONDUPDATER trojan. In addition, attackers leaked the web shells HYPERSHELL and HIGHSHELL, known by Palo Alto Networks as TWOFACE, as well as the FOXPANEL phishing software. Lab Dookhtegan also released the identities of attackers that it claimed belonged to APT34 (see Figure 2). Additional messages posted a Python-based DNS hijacking tool named WEBMASK_DNSPIONAGE and files containing compromised account information from targets of APT34 (see Figure 3). Also, Lab Dookhtegan created and released PDF documents where the attackers' photos, phone numbers, email addresses, and social media accounts were leaked (see Figure 4).

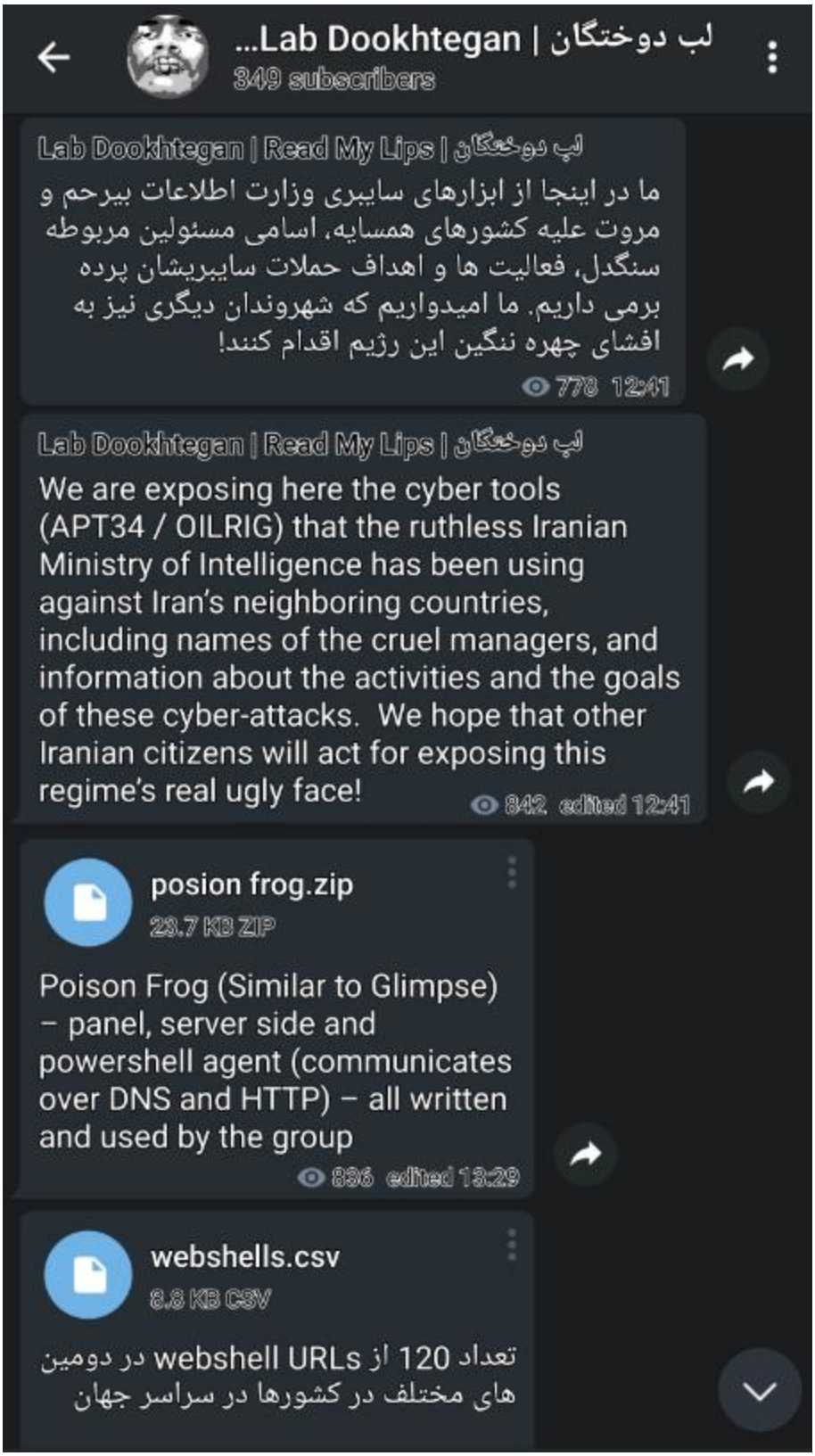


Figure 1. Screenshot of Telegram channel Lab Dookhtegan

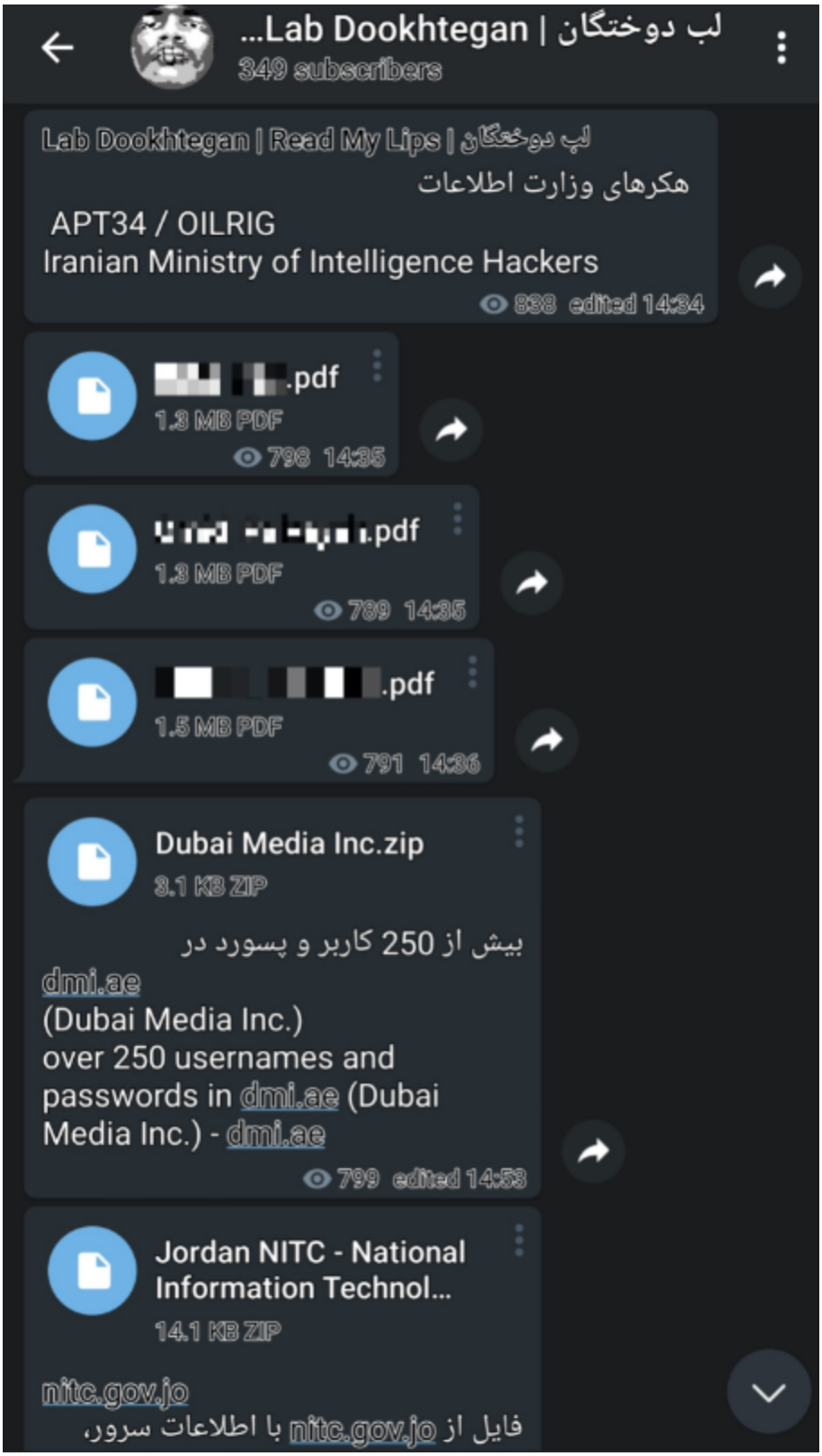


Figure 2. Screenshot of compromised APT34 attacker identities

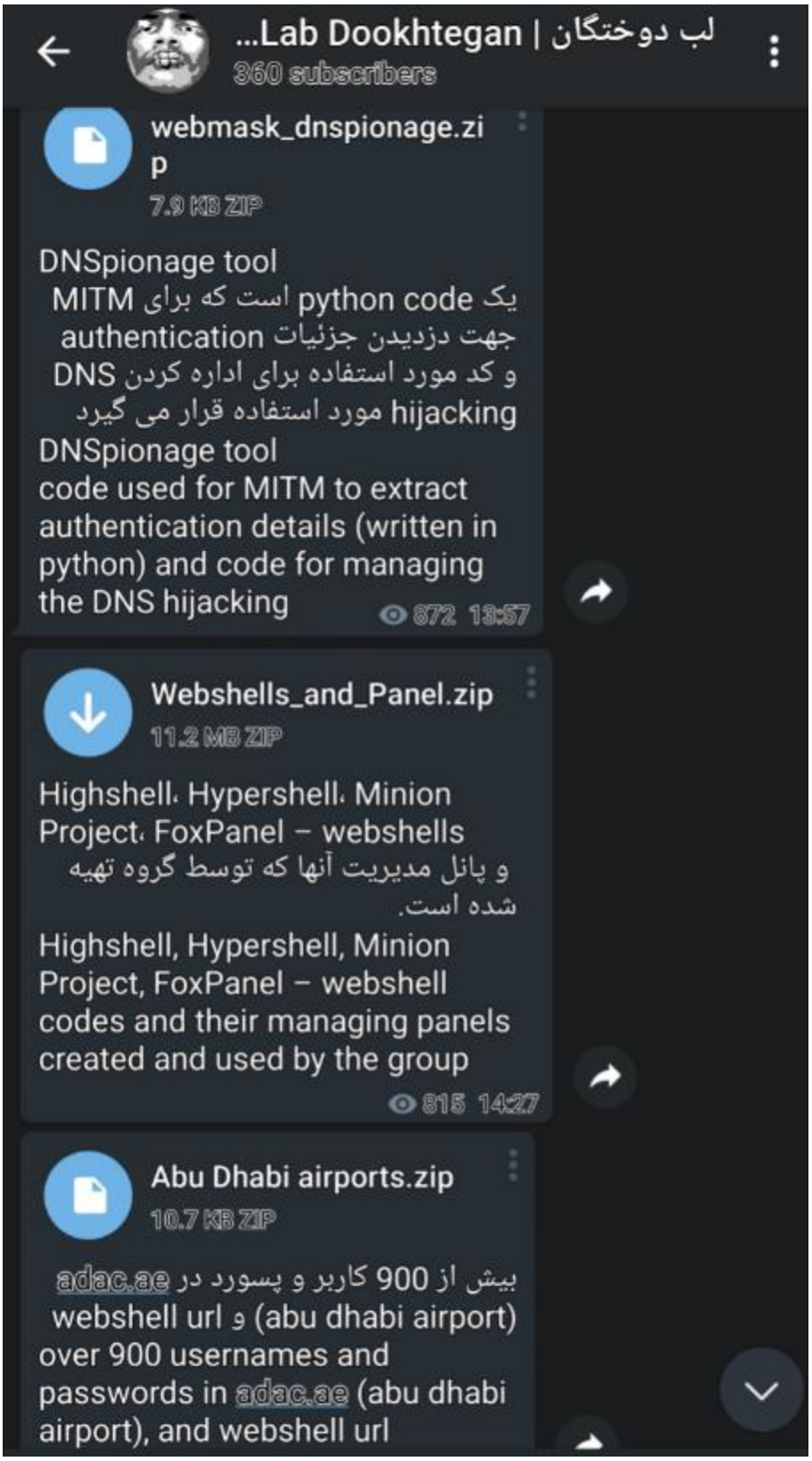


Figure 3. Screenshot of compromised APT34 tools

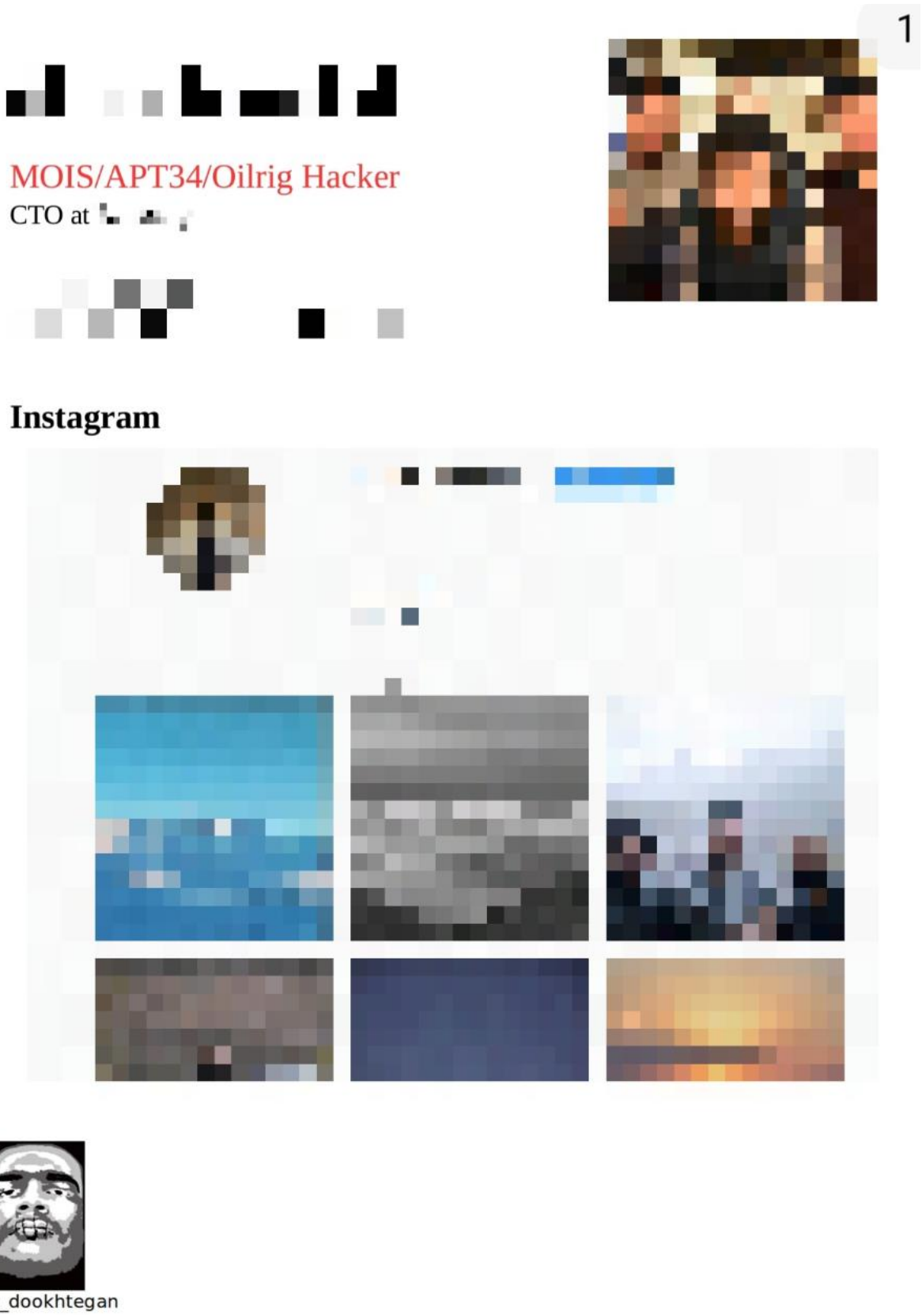


Figure 4. Screenshot of Lab Dookhtegan document exposing an APT34 attacker's identity

APT35. APT35, also identified by the names Operation Saffron Rose, Ajax Security Team, Flying Kitten, Newscaster, Gholee, Rocket Kitten, Operation Woolen-Goldfish, Thamar Reservoir, Charming Kitten, and Magic Hound, is an Iranian cyber espionage group with operations that are estimated to have begun in 2010. Over time, the wide range of cyberattacks, targeted nations and industries, and toolkits used by APT35 have led some cybersecurity professionals to the conclusion that it is not one singular group, but multiple cyber threat actors leveraging shared resources and partially composed of the same team members. Other professionals classify APT35 as a single group. This study will refer to APT35 as a singular entity, and look at the differentiations of opinion further into the research.

Villeneuve, Moran, Haq & Scott (2013) first wrote that APT35 was using a spear phishing by way of emails and private messages on social media to entice targets into entering illegitimate websites, which were based on professional conferences and events. The websites would then inform the user that they required the installation of additional software to access the site, the likes of which was actually malware. At this time, they also set up illegitimate websites to imitate legitimate services such as Virtual Private Networks (VPN), and used these websites to facilitate credential phishing against targeted users. During this time, APT35 also utilized a family of data exfiltration malware referred to by the attackers as Stealer. The Stealer malware family originated from a singular executable file that would be dropped onto a system, at which point it would insert additional malicious files. Each malicious file provided its own data exfiltration function, and attackers were capable of encryption, keylogging, data exfiltration based on File Transfer Protocol (FTP), extraction of browser Uniform Resource Locators (URL) and Internet Explorer (IE) accounts, and capturing screenshots. Command and Control (C2) infrastructure for the attacks consisted of multiple domain names and email addresses used to

register and create websites illegitimately associated with legitimate events across the aerospace and defense industries.

APT35 later emerged as a conglomerate of over 2000 fake social media personas, in a campaign dubbed Newscaster by iSight Partners Inc. (2014). The Newscaster campaign involved utilizing these personas, which spanned across multiple platforms such as LinkedIn, Facebook, Twitter, and Google, to target senior military and government officials in the US and Israel. After having established contact with their target, threat actors would phish their login credentials by linking them to one of several illegitimate services made to appear as legitimate login pages for sites like Yahoo, Google, and Outlook. These illegitimate services were actually connected to the website, NewsOnAir.org, an elaborate online news organization created by APT35 to provide infrastructure with which to host their attacks, as well as provide pretexting for their social media personas, many of which were purported journalists for the online news service. From an offensive perspective, infrastructure would be used to leverage this credential-theft, as well as to insert an Internet Relay Chat (IRC) bot-based malware onto the targeted system. The IRC bot could then be leveraged by the attackers to download remote files, execute files, and search infected disks.

The same year, cybersecurity firm Clearsky wrote a report entitled Gholee (2014), in which it publicized another spear phishing campaign by APT35. The spear phishing campaign, utilizing a malware called GHOLEE as its payload, was conducted parallel to the 2014 Israel-Gaza conflict dubbed Operation Protective Edge, and utilized malware contained in a file named ‘Operation Protective Edge.xlsb’. The malware, hidden in the macros of a weaponized Microsoft Excel document, prodded the user to enable macro-based content, and thereby execute the

malware. Once activated, the malware enables data exfiltration through the Secure Socket Layer (SSL) protocol over port 443, using an expired digital certificate to feign secure authentication.

Later, Pernet and Lu (2015) published Operation Woolen-Goldfish, a Trend Micro Inc. cybersecurity report detailing further use of the GHOLEE malware. In it, the authors critiqued the attackers' use of macro-based protocols to deliver GHOLEE, underscoring that while the Gholee malware itself is relatively advanced, the use of weaponized, macro-embedded documents to deliver attack payloads is considered amateur. They also noted that GHOLEE was itself a modified version of a legitimate, high-end penetration testing tool manufactured by the cybersecurity company Core Impact.

The Operation Woolen-Goldfish report also detailed a spear phishing campaign by APT35, in which attackers masqueraded as recognized Israeli engineers and defense officials in order to con targets into opening malicious executable files. The executable files were stored on OneDrive, Microsoft's online cloud storage system, and were disguised to resemble Microsoft Office files, such as PowerPoint. However, the files maintained there .exe file extension, denoting executable content, and would silently run keylogging malware named CWOOLGER in the background of the computer once opened. This keylogging malware was linked to an FTP server which was used as C2 infrastructure for exfiltration of logged data (Pernet & Lu, 2015).

Clearsky (2015) went on to publish a report on Thamar Reservoir, another APT35 cyberattack campaign characterized by extreme persistence against singular targets. Thamar Reservoir is presumed to have begun when attackers breached the email account of an unnamed individual in touch with several Israeli researchers. After this initial compromise, the attackers created a second email address very similar to that of the unnamed individual, and sent follow-up emails to the researchers that stemmed from conversations begun by the former, legitimate email

account. These emails contained a weaponized Microsoft Excel Document, with malicious macros that dropped executable and batch files onto the host machine when enabled. The batch file created a registry key within the system that would run the executable file every time the computer started. This executable file is then used to remotely download additional malware files, such as the CWOOLGER keylogger used in Operation Woolen-Goldfish.

In other instances, the attackers created email addresses that strongly resembled those of a target's actual contacts. Another spear phishing tactic leveraged by the attackers involved spoofing the email address for BBC Persian Television and requesting that their target access a linked Adobe Acrobat .pdf file. Once accessed, the .pdf file would redirect the target to a fake Google Drive login page manufactured by the attackers. This fake login page was mirrored to resemble the web page of the real Google Drive service, and would harvest the credentials of the users who input their information into it (Clearsky, 2015).

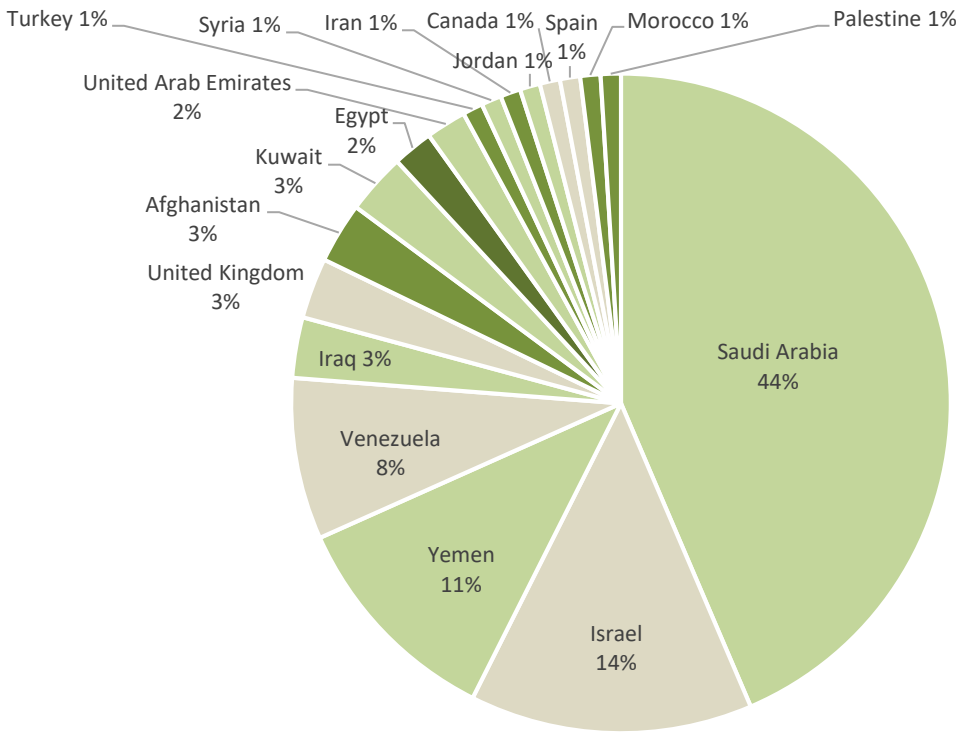
The Thamar Reservoir campaign also continued the attackers' pattern of fabricating professional events. Clearsky (2015) noted in their report that APT35 managed to compromise a legitimate Israeli research institute, and subsequently send emails from the email address of that institute, inviting targets to attend a virtual Iranian-Israeli forum. The Iranian-Israeli forum appeared to be linked to other legitimate services such as Google, Yahoo, and AOL accounts through federated identity. However, this was a ruse; clicking on the login icons for any of the services redirected the target to an illegitimate login page that was tailored to appear as though it belonged to the user's account. These illegitimate login pages were used in conjunction with other imitated services to obtain user login credentials.

Other spear phishing methods were used in Thamar Reservoir. One of these was vishing, where a target was conned into revealing their login credentials through a phone conversation.

Another instance involved an attacker directing targets to an imitation YouTube login page, where the target would unwittingly enter their login credentials before being directed to the legitimate YouTube site. Yet another tactic attempted to abuse the account recovery procedures of Google, Facebook and Yahoo to retrieve login credentials. The attackers also persistently contacted one of the central targets of the campaign through private messages on Facebook, requesting personal information throughout conversations conducted in Persian. A distribution chart of targeted countries based on over 500 attacks was published within the report (see Table 1).

Table 1.

Partial List of Target Countries



Source. Published by ClearSky Cyber Security (2015)

Thamar Reservoir was not without its shortcomings. Authors of the report by Clearsky (2015) note frequent errors in the use of the Hebrew and English language that marred the social

engineering pretexts leveraged by the attackers. One target noted that vishing attempts against them were conducted by an individual speaking “bad English,” and both English and Hebrew-language phishing emails contained multiple linguistic errors, despite purporting to come from professional sources.

At this point in time, Pernet and Sela (2015) released an analytical report characterizing APT35 by its dual use of simple, custom-developed tools, alongside more advanced, publicly available ones. They went on the highlight the frequent typos and grammatical mistakes in the illegitimate content created for its credential phishing operations, which made their attacks more readily identifiable. The authors echoed analysts before them in emphasizing the immense persistence with which APT35 conducted its cyberattacks, detailing that individuals were the target of spear phishing attempts across multiple mediums on a daily basis, with different pretexts and techniques creating a near inevitability that compromise would eventually succeed.

Check Point Technologies (2015), in a subsequent report entitled Rocket Kitten, published the results of their own reconnaissance operation that sought to engage APT35’s C2 infrastructure. This reconnaissance operation had been immensely successful due to severe misconfigurations of web servers used to host the cyberattacks. This failure resulted in the authors’ discovery of a table based within the C2 infrastructure, detailing over 1842 different email addresses targeted throughout cyber warfare operations occurring from August 2014 to August 2015. The authors wrote that a separate part of the table, entitled “projectlogs”, contained log entries of all incidents involving a target accessing a phishing page.

In the report, Check Point Technologies (2015) strongly criticized the C2 infrastructure used to support the cyberattacks conducted. The aforementioned misconfiguration that allowed analysts to enter and peruse the contents of the C2 infrastructure resulted from the attackers’ lack

of understanding as to how XAMPP web servers were set up, therefore the web servers being used by various spear phishing campaigns was set to allow root access with no password requirement. This meant that any user could log directly into the attackers' C2 infrastructure and browse its full contents at will. Authors of the report also underlined the fact that the attackers had infected their own computers with the CWOOLGER keylogging malware, in what is believed the have been early test runs. However, because the attackers had failed to ever remove the CWoolger malware from their computers, the C2 infrastructure also contained their own keylogged information. This led Check Point Technologies to discover the name of a key member of APT35, Yaser Balaghi, who had been operating under the pseudonym Wool3n.H4T.

Check Point Software Technologies (2015) also presented a threat intelligence report in which it provided additional details on past activities by the group. In this report, the following custom-made tools were attributed to APT35s cyber arsenal:

1. CWOOLGER – A keylogger written in C++ that exfiltrated logged data to an FTP server
2. GHOLEE – A repurposed penetration testing tool by Core Impact that granted attackers remote access and network pivoting capabilities
3. FIREMALV – A credential theft tool written in the Microsoft .NET Framework, which retrieved passwords from Firefox browser storage
4. .NETWOOLGER – A keylogger written in the Microsoft .NET Framework, that functioned almost identically to CWoolger
5. MPK – A multipurpose RAT that allowed keylogging, command execution, screenshot capture and traffic monitoring

Also, the same report by Check Point Software Technologies (2015) wrote that the open-source tools Metasploit, SQLMap, Acunetic, Netsparker, and WSO Web Shell were used to scan and attack targets.

Check Point Software Technologies (2015) claimed that there was no concrete evidence linking APT35, which they referred to as Rocket Kitten, to either Operation Saffron Rose or Newscaster. However, other cybersecurity firms persist that the groups are one in the same (FireEye, 2018).

Two years later, Lee and Falcone (2017) published on a Palo Alto Networks threat intelligence blog that a cyberattack campaign dubbed Magic Hound had been discovered, and that link analysis of this campaign revealed strong ties to APT35. Cybersecurity firm Clearsky (2017) reiterated this link in their own report, and stated that their own findings supported the connection. The cyberattack campaign was estimated to have begun in mid-2016, and utilized a collection of tools previously seen in other APT35 attacks, including weaponized Microsoft Office documents embedded with malicious macros, IRC bots, malicious executable files, and an open-source Python-based Remote Access Tool (RAT) named Pupy. There was also a new family of malware named MAGICHOUND. Analysts at Palo Alto Networks listed them as follows:

1. MAGICHOUND.ROLLOVER - A Metasploit-based Meterpreter payload.
2. MAGICHOUND.FETCH – A persistent access tool used to load secondary payloads from C2 infrastructure, and to run PowerShell commands to execute shellcode. This tool used Advanced Encryption Algorithm (AES) to embed its strings as an anti-analysis technique. Analysts at Palo Alto Networks were able to reverse engineer this after discovering that the obfuscation processes all utilized the same password.

3. MAGICHOUND.DROPIT – An executable dropper file that builds an additional executable file through decoding base64-encoded data embedded within itself, then arranging it into a functioning order. This tool also functioned as a binder tool, combining decoy executable files with malicious ones in order to obscure malicious processes into the background of the computer.
4. MAGICHOUND.RETRIEVER – A Trojan malware installed through MAGICHOUND.DROPIT, written in the Microsoft .NET Framework, which pulls secondary payloads from existing C2 Infrastructure.
5. MAGICHOUND.LEASH – An IRC bot linked to an IRC C2 server, capable of command execution, remote file download, and both file and directory deletion. Authors underscored that this IRC bot functions similarly to the ones used in the Newscaster campaign.

Clearsky (2017) differentiates APT35 as a group of distinctly separate cyber threat actors throughout the timeline between 2010 and 2015, positing that FireEye's Operation Saffron Rose report concerned a threat actor called Flying Kitten, and that another threat actor known as Rocket Kitten would emerge several months later. Clearsky also highlights that strong ambiguities exist that blur the presumed cyber threat actors into a singular entity, noting both the singular timeline as well as shared code used in cyberattacks. They also state that, due to the obscurity surrounding the ecosystem of Iran's cyber warfare operations, it is possible that the two groups share the same members, and note that significant overlaps exist between the two entities.

FireEye (2018), in its annual cybersecurity trends report, continues to refer to APT35 and its associated operations as a single threat actor.

Cleaver. The Cleaver team was named by Cylance (2014) in their comprehensive report on Operation Cleaver, a cyber espionage campaign beginning in 2013, conducted against aerospace, defense, education, government, oil and gas, technology, telecommunications, and transportation industries, ranging within 16 different countries, spanning across three continents. Authors of the Operation Cleaver report asserted that the Cleaver Team was a distinct group in and of itself, whose ranks included both members of previous Iranian cyber threat actors and new recruits. The Cleaver team was referenced as Threat Group 2889 (TG-2889), and later as Cobalt Gypsy, by Dell Secureworks Counter Threat Unit ("Suspected Hacker Group Creates Network of Fake LinkedIn Profiles", 2015).

Cylance (2014) recorded that, in order to establish initial compromise, attackers in Operation Cleaver utilized a complex spear-phishing campaign. The campaign was pretexted by a job opportunity, in which targets were made to believe they were being considered for a position with a major corporation, such as Teledyne or Northrop Grumman. The Cleaver team orchestrated this pretext through email and would eventually lure their targets to a third-party resume creator website and instruct them to download software required to submit their resume for the job position. Although the website and software referenced by the Cleaver team was legitimate, the targets had been linked to an illegitimate website created for the purposes of these cyberattacks, which was visually identical to the original website. The software on this illegitimate website was also a copy of the legitimate resume creation software, and created a backdoor named TINYZBOT in the background of the otherwise seemingly function application.

Cylance (2014) analysts noted that these spear phishing techniques were bulwarked by their underlying context: if the targeted individual were to suspect they had downloaded a

malicious application, they may have been less inclined to reveal this information to their superiors, as doing so would reveal that they had been applying to another job in the first place.

A second method used to achieve initial compromise was SQL injection (SQLi). The Cleaver team was noted to have double-encoded its SQLi payloads, which allowed the attacks to bypass Web Application Firewall (WAF) filters (Cylance, 2014).

For successful privilege escalation, the Cleaver team leveraged known exploits such as Common Vulnerabilities and Exposures (CVE) 2010-0232, in order to establish kernel-level access to unpatched Windows systems. CVE are dictionary-style references to publicly known cybersecurity threats. The Cleaver team also pivoted across target networks using the publicly available Mimikatz tool and Windows Credential Editor to perform cached credential dumping, whereby network access credentials already stored on the system's cache are extracted and utilized for additional means of authentication. The use of the open-source Mimikatz application was augmented by the attackers, who created two automated tools in C#, named ZHMIMIKATZ and MIMIKATZWRAPPER, in order to streamline the Mimikatz functions that most pertained to their operational goals (Cylance, 2014).

Once cached credentials had been successfully captured, the Cleaver team used the Windows tool PsExec to move laterally from computer to computer, and employed the Net Crawler (NetC) application to garnish more cached credentials from the systems it gained access to. This combined set of cached credential dumping tools allowed attackers to compromise entire networks (Cylance, 2014).

The Cleaver team also created a C-language tool named JASUS, made to facilitate Address Resolution Protocol (ARP) cache poisoning, but Cylance (2014) authors criticized it as below the standard of many publicly available tools that serve the same purpose, and offer more

advanced features. Despite this, the tool did serve a purpose; having been custom made by the Cleaver team, JASUS was relatively difficult to detect by antivirus (AV) software that relied on known malware signatures to recognize cyberattacks. The publicly available Cain & Abel toolkit was used to extract credentials from network-based caches when no AV was present.

In order to exfiltrate data from compromised systems, the Cleaver team leveraged C2 infrastructure based on anonymous FTP to send large volumes of data through command line functions already available on their targets. Cylance (2014) authors underscored the versatility of this tactic, as it employed a "living off the land" approach by utilizing the system's own data transfer methods, and not requiring additional malware that would have increased detectability. The attackers also used the publicly available NetCat tool as a means of data exfiltration, as well as a tool to establish a reverse shell for remote control over the system. Later in their campaign, the Cleaver team replaced NetCat with ZHCAT, a custom-made tool mimicking the required functions of NetCat, but adding data obfuscation and encryption techniques to mitigate detection.

Other strategies to achieve data exfiltration included the use of the Secure Socket Shell (SSH), an encrypted tunneling protocol that the Cleaver team called upon through the PLink utility provided by the PuTTY suite of SSH-based tools. The attackers used PLink to connect to compromised systems via Remote Desktop Protocol (RDP), allowing for visually-oriented data exfiltration and remote control of the systems. Cylance (2014) also reported that earlier in Operation Cleaver, the attackers used the Simple Mail Transfer Protocol (SMTP) to exfiltrate data, attaching compromised files to emails that had been made to resemble common spam.

To maintain persistent access to the network, the TINYZBOT backdoor was created in the initial stages of system compromise. Developed in C# by the Cleaver team, TINYZBOT became a key utility within the course of the cyber espionage operations, expanding in function

to allow for FTP and SMTP-based data exfiltration, screenshot capturing, keylogging, HTTP-based C2 communications, arbitrary code execution, browser-based password extraction, AV detection, the ability to disable Avira AV products, and the modification of executable files (Cylance, 2014).

One year after the publication of Cylance's 2014 Operation Cleaver report, Dell's Secureworks Counter Threat Unit provided a follow up to the original findings in which they identified a small network of regularly updated, fake social media personas used for social engineering purposes. These personas were based off of the LinkedIn platform, and were believed to be used to build credibility via professional endorsement ("Suspected Hacker Group Creates Network of Fake LinkedIn Profiles", 2015). In 2017, Dell published another follow up, renaming the group Cobalt Gypsy and tying it to a spear phishing campaign being conducted via LinkedIn. The activity presented during this point in time aligned with the same targets and sectors from the 2013 campaign, and even still utilized the same pretexting methods employed by the earlier phases of the operation. It was also underscored that the Pupy RAT tool used by APT35 was being employed by the Cleaver team as a means of initial compromise (The Curious Case of Mia Ash, 2017).

TEMP.Zagros. Lancaster (2017), on behalf of Palo Alto Networks, published that a spear phishing campaign targeting primarily Middle Eastern targets had been leveraging a set of weaponized Microsoft Office documents with malicious macros to distribute a PowerShell-based backdoor. Nation-state targets included Georgia, India, Iraq, Israel, Pakistan, the KSA, the United Arab Emirates (UAE) and the U.S. Palo Alto Networks named the group MuddyWater, but later iterations of reports by other cybersecurity vendors would use the name TEMP.Zagros.

Weaponized documents used by TEMP.Zagros were made to resemble official government publications, and bore the emblems of each respective nation when opened. Users would be prodded by text on the front page of the document to fully enable the document, which would then activate the malicious macros and establish the PowerShell-based backdoor (Lancaster, 2017). The next year, FireEye published that these TTPs had been updated, and the weaponized documents had become exceptionally more refined. Government emblems were updated to more accurately reflect individual agencies. Also, the use of in-document text to requested enabled access from the user was replaced by a separate window overlaying the document, which blurred a very convincing template in the background below it. (Singh, Jallepalli, Londhe & Read, 2018).

Analysts at FireEye also provided an in-depth look at the PowerShell-based backdoor, which had evolved to add in obfuscation elements to hide its functionality from reverse engineers and AVs. Obfuscation was achieved using character replacement mechanisms, environmental variables, and XOR encoding using a single-byte key. The PowerShell script allowed attackers to retrieve a compromised system's IP address, operating system (OS) name and architecture, computer name, domain name, and the username. It proceeded to establish persistence by registering the targeted system to corresponding C2 infrastructure, and then allowed for post-exploitation activities such as screenshot capture, remote file upload, and remote code execution. The script could also detect security tools capable of hindering its operation, and shut down the system in the event that a relevant security tool was discovered. Messages between the compromised system and the respective C2 infrastructure were encrypted and decrypted using the Rivest-Shamir-Adleman (RSA) algorithm. Although it was not at all delved into within the

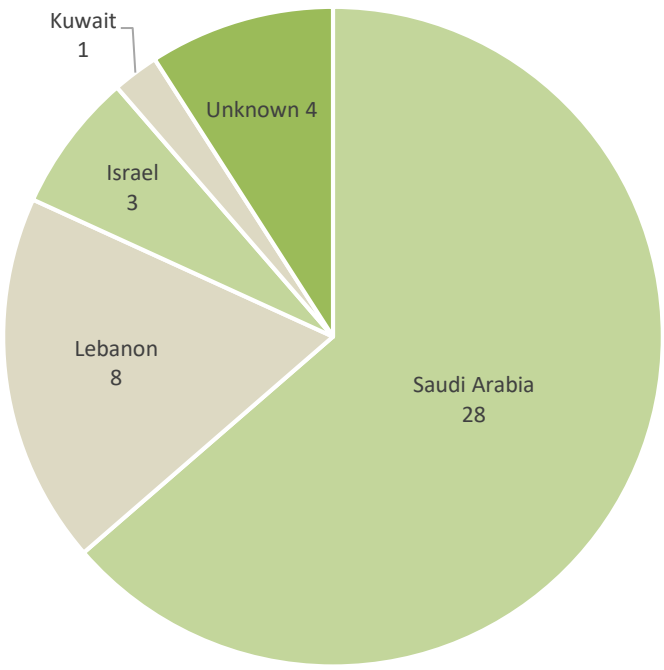
report, authors noted that the PowerShell backdoor was capable of wiping the drives on a compromised system (Singh, et al., 2018).

Approximately one year later, Villaneuva and Co (2018) published that TEMP.Zagros had been observed using the similar weaponized Microsoft Office documents to distribute a more advanced PowerShell script. The weaponized documents functioned in the same manner as previous iterations, but resembled rewards or promotions by third-party companies. The PowerShell-based backdoor had been heavily modified, and was actually one original script that executed into a second PowerShell script after having been fetched from the contents of an encoded malicious document. The resulting backdoor communicates with C2 infrastructure to establish persistence, and then allows attackers to collect browsing histories and browser-based passwords, execute shell commands, enable keylogging, capture screenshots, gather system information, and initialize Domain Name Service (DNS) sessions. The authors concluded their research by underscoring that TEMP.Zagros was capable of self-advancement, augmenting their own TTPs to increase the effectiveness of their operations.

Leafminer. In July 2018, Symantec published that a Leafminer was an Iranian cyber espionage group conducting campaigns against financial, government, petrochemical, transportation, and other industry sectors throughout the Middle East region, specifically the KSA, Lebanon, Israel, and Kuwait. Authors highlighted that an investigation into Leafminer's activities revealed a publicly accessible, web-based C2 infrastructure that stored 112 files, composed of malware, payloads, toolkits, and log files retrieved from cyberattacks. Research into this C2 infrastructure linked its origin to members of the Iranian hacking forum Ashiyane, in addition to the cyber threat actor Sun Army ("Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions", 2018).

Table 2.

Location and Number of Computers Compromised by Leafminer



Source. Leafminer: New espionage campaigns targeting Middle Eastern Regions (2018)

Leafminer established initial compromise through watering hole attacks, known network vulnerabilities, and dictionary attacks against network login services. Watering hole attacks involved planting malicious JavaScript code into legitimate websites, which was used to steal Server Message Block (SMB) credentials that would then be brute-forced offline. Symantec analysts note that this technique seems to have been mimicked from Dragonfly, a Russian cyber threat actor who, one year previous, was successfully employing the tactic against its own targets ("Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions", 2018).

Vulnerability scans performed by Leafminer indicate that the group was searching for the potential to leverage publicly-known exploits, such as SMB server vulnerabilities described in

Microsoft Security Bulletin MS17-010, the Heartbleed vulnerability known as CVE-2014-0160, and the EternalBlue exploit popularized by unrelated ransomware campaigns that took place between 2017 and 2018 ("Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions", 2018).

Evasion techniques leveraged by Leafminer strongly suggest that it monitored developing TTPs within the world of cybersecurity. After the presentation of Process Doppelgänging at the 2017 Black Hat EU conference, Leafminer swiftly adopted it into its arsenal. Process Doppelgänging involves the use of New Technology File System (NTFS) transactions to subtly alter a malicious process occurring in the background of a system. Symantec analysts noted that the code published by the authors of this technique seems to have been almost directly copied by Leafminer during the course of its cyber espionage operations ("Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions", 2018).

Two custom-made pieces of malware were utilized by Leafminer, both which indicated a preference the Microsoft .NET Framework. This malware included BACKDOOR.SORGU, which provided remote access via a shell command script, and TROJAN.IMECAB, which established persistence remote access through the creation of a privileged guest account onto the system. Leafminer also incorporated a modified element of the Inception Framework toolkit, which was released by the threat actor Shadow Brokers, into its cyberattacks ("Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions", 2018).

Authors at Symantec assessed that Leafminer was a relatively inexperienced APT, who relied on TTPs already popularized by more advanced threat actors, and whose C2 infrastructure was ultimately marred by poor operational security (OPSEC).

APT39. At the time of this writing, APT39 is a relatively new threat actor, having been reported by FireEye's Threat Research blog in January 2019. Authors of this report stated that APT39 is an Iranian cyber espionage APT whose theft of personal information has been linked to disruptive and destructive attacks and influence operations, emphasizing that their activities likely support Iranian intelligence operations, as well as facilitate future cyber warfare campaigns through the use of strategic information gathering. The report articulates that APT39's primary focus on attacking telecommunications and travel sectors lends credence to the support of surveillance and monitoring operations, noting that data exfiltration performed by the group typically targets proprietary and customer data from these industries, sometimes against specific individuals, with additional measures being taken to establish persistent access for future campaigns (Hawley et al., 2019). An annual trend report by FireEye (2019) also underscored APT39 was targeting the government sectors and transportation industries of Israel and Kuwait.

APT39 shares strong resemblances with APT34. Both leverage similar spear phishing campaigns to deliver malware, use the same POWBAT backdoor in their operations, and name C2 infrastructure similarly. Despite this, authors of FireEye's report assert that the two APTs remain distinct from one another, and that these comparisons indicate that APT39 and APT34 may work together (Hawley et al., 2019).

To achieve initial compromise, APT39 delivers the POWBAT backdoor through spear phishing emails, often in the form of a malicious attachment or hyperlink. The domain names used throughout APT39's operations mirror legitimate web services that align with the targeted organization. Attackers have also demonstrated the capability to steal credentials that are then used to gain access to external Outlook resources (Hawley et al., 2019).

Custom backdoors such as SEAWEED, CACHEMONEY, and a second variant of POWBAT are used gain presence within a newly compromised environment. Attackers use publicly available tools such as Mimikatz, Ncrack, ProcDump, and the Windows Credential Editor to conduct privilege escalation. Lateral movement throughout the network is achieved using other publicly available tools and open-source standards, including RDP, SSH, PsExec, RemCom and xCmdSvc, and a small suite of custom tools, named BLUETRIP, REDTRIP and PINKTRIP, all which create SOCKS5 proxies to link compromised systems to one another.

Lebanese Cyber Espionage Campaigns

Lebanese Hezbollah. According to Cilluffo (2012), Hezbollah began cyber warfare operations in June 2011 through the establishment of a companion organization named Cyber Hezbollah. At the time, Hezbollah's priorities consisted of preparing and mobilization of offensive cyberspace forces, as well as conducting open-source intelligence through social media to gain strategic insight on its adversaries. Four years later, in a testimony to the U.S. House of Representatives, Cilluffo (2016) stated that Hezbollah was connected to SHAMOON, Iran's destructive cyber operation against the KSA's Saudi Aramco and Qatar's RasGas corporations.

Check Point Software Technologies (2015) released a report on a cyber espionage operation coined Volatile Cedar, in which a politically motivated set of attacks originating from Lebanon had successfully penetrated Israel's defense sector since at least 2012. Regional analysts and security professionals have attributed these activities to Hezbollah ("The Cyber Party of God", 2018).

Cyberattacks by Volatile Cedar typically targeted public web servers, and conducted vulnerability scanning against these servers as an active reconnaissance technique. After finding a vulnerability, attackers would then target the web server with shell code injection to

compromise it. With the compromised web server in hand, the Volatile Cedar operation would seek to deliver a Trojan malware directly into the organization's internal servers. This malware, dubbed EXPLOSIVE, connected to C2 infrastructure to send remote commands across all compromised targets (Check Point Technologies, 2015).

EXPLOSIVE has been underscored for its built-in evasive capabilities, achieved through a wide set of characteristics built into its design. These include its dedication to monitoring memory consumption, which stifles server administration tools that my otherwise have been alerted by it, and separation of its irregular functions into a separate Dynamic Link Library (DLL), which largely obscured it from behavior-based detection. In addition, attackers behind EXPLOSIVE frequently released new variants of the malware in order to circumvent signature-based detection, and even timed these releases with publicly known AV signature updates. Variants of EXPLOSIVE were further augmented based on the target being attacked. Communications between EXPLOSIVE and its respective C2 infrastructure were heavily obfuscated to appear as ordinary network traffic, and contained built-in functions to continually check whether or not communications were being targeted by a detection system (Check Point Technologies, 2015).

For additional obfuscation, EXPLOSIVE leveraged a custom ASCII encoding algorithm, as well as a second custom encoding algorithm for generated network traffic. Authors stated that the algorithms used by EXPLOSIVE to communicate with C2 infrastructure were exceptionally advanced, and included a large quantity of branches and loops that serve no purpose other than to further complicate the procedure (Check Point Technologies, 2015).

EXPLOSIVE communicated with C2 infrastructure through a multi-faceted, layered process, which involved a core set of C2 servers whose addresses were periodically changed by a

secondary set of static C2 servers, and a third set of C2 servers that communicate with EXPLOSIVE in the event that the core C2 servers are unresponsive. This triage of C2 infrastructure was further diversified by origin; while the attackers were in possession of some of the C2 servers, others were previously compromised systems or publicly hosted platforms. C2 infrastructure was capable of retrieving browser history, stored passwords, registry information, current running processes, and individual files from a compromised system, and could also run remote commands on the system's command line (Check Point Technologies, 2015).

Check Point Technologies (2015) emphasized that the first C2 servers utilized within the operation were hosted by a prominent Lebanese hosting service, a characteristic which it deemed highly irregular. They further underscored that OPSEC failures behind Volatile Cedar led to the discovery of one attacker's identity. Authors of the report did not disclose the identity of this individual, but noted their apparent history of political activism within the country.

Dark Caracal. Operating since 2012 and publicly exposed in 2018, Dark Caracal is a cyber threat actor whose activities are directly attributable to Lebanon's General Directorate of General Security (GDGS), headquartered in Beirut. One distinct factor immediately setting the group apart from other threat actors is its strong focus on mobile-based attack platforms, including malicious Android applications used to surveil targeted mobile systems. This attack vector has allowed the group to compromise an expansive number of systems, with targets ranging across military, government, medical, academic, and commercial enterprise sectors. It also affected a wide scope of countries; successfully compromised targets resided in China, France, Germany, India, Italy, Jordan, Lebanon, Nepal, the Netherlands, Pakistan, the Philippines, Qatar, Russia, the KSA, South Korea, Switzerland, Syria, Thailand, the US,

Venezuela, and Vietnam. Authors of Lookout's report on Dark Caracal have noted that the group simultaneously runs approximately six cyber espionage campaigns (Blaich, et al., 2018).

Initial compromise by Dark Caracal followed standardized procedures. Phishing messages were used throughout social media sites and distributed over WhatsApp messages in order to drive targets to a watering hole website where malicious Android applications could be downloaded. These applications posed as popular chat services such as Signal, WhatsApp, and Telegram, and contained a surveillance-based malware dubbed PALLAS. Additional phishing campaigns leveraged illegitimate copies of websites such as Facebook and Google to con users into inputting login credentials (Blaich, et al., 2018).

Weaponized Microsoft Word documents with malicious macros were also used to compromise targeted systems. These documents used overlaid messages instructing users to open the file through their local Microsoft Office program, and to enable editing so as to activate macro-enabled content (Blaich, et al., 2018).

Mobile systems infected with PALLAS were largely controllable by the malware, and could be leveraged to take pictures from the device's front or rear camera, retrieve GPS coordinates, scan surrounding Wi-Fi access points (AP), upload specific files, and download additional applications (Blaich, et al., 2018).

Against desktop computers, Dark Caracal leveraged a known family of RAT malware known as BANDOOK. Variants of BANDOOK used by the attackers were signed with a valid SSL certificate, which had been issued by Certum Certificate Authority (CA). Authors of the Dark Caracal report also noted that a new Java-based RAT malware, dubbed CROSSRAT, was custom developed by the APT. CROSSRAT was able to control file systems and take screenshots through a computer's webcam (Blaich, et al., 2018).

Data exfiltrated by Dark Caracal's mobile-based operations included personal text messages, password PINs, travel documents, airline receipts, contact lists, call logs, browsing history, account login credentials, audio recordings, photos, and system information. When targeting desktop systems, successful compromise allowed for the exfiltration of captured screenshots, Skype logs, photos, iPhone backups, and all Windows file and folder listings (Blaich, et al., 2018).

C2 infrastructure utilized by Dark Caracal's cyber espionage operations was largely hosted by the web hosting service Shinjiru. A single C2 server is used to host the watering hole website advertising malicious Android applications. Several other servers were used for social media-based phishing websites. Separate C2 infrastructure was leveraged for Windows-based cyberattacks, and authors of the Lookout report wrote that this infrastructure had been in use much longer than the servers hosting malicious Android applications (Blaich, et al., 2018).

Palestinian Cyber Espionage Campaigns

Molerats. Molerats, also identified by the names Gaza Hackers Team, Gaza Cybergang, and DustySky, is a cyber threat actor with recorded cyberattacks against organizations in Israel, Egypt, the KSA, Iraq, and the United Arab Emirates, as well as the US and the United Kingdom (UK). Clearsky (2016) identified that its operations originated from the Gaza Strip, after analyzing malware samples used by the attackers.

Villeneuve, Haq and Moran (2013) identified early activity by Molerats which they named Operation Molerats, in which the group leveraged POISONIVY, a popular RAT backdoor that had been traditionally associated with Chinese cyber espionage campaigns. The authors noted that previous cyberattacks by Molerats in 2012 used publicly available RAT utilities to exploit targets, but that their strategies became reliant on the POISONIVY tool in 2013.

Spear phishing campaigns were employed to gain initial compromise over targeted systems, with attackers delivering weaponized Roshal Archive (RAR) files, either attached directly to emails or hosted on DropBox. The emails would attempt to take advantage of trending regional news by sending the contents of Arabic, Hebrew, and English-language news articles within compressed Microsoft Word documents, using titles of these news events as the email subjects. Once opened, these files would activate the underlying PIVY malware, allowing attackers access to the targeted system. At the time of writing, the authors noted that 15 samples of PIVY linked to Operation Molerats and the Molerats through common C2 infrastructure (Villeneuve, et al., 2013)

Clearsky (2016) later published a two-part report detailing Operation DustySky, a cyber espionage campaign beginning in 2015 where Molerats targeted government, aerospace, defense, financial, news, and information technology (IT) sectors with a malware, dubbed DUSTYSKY, that was hidden behind Hebrew, Arabic, and English-language content. This content was not tailored to individual targets, and therefore not within the definitions of spear phishing. Similar to the activities in Operation Molerats, Molerats place news content into malicious RAR files in an attempt to lure targets to opening the weaponized documents. The malware would be stored either on C2 infrastructure owned by the attackers, or on public file sharing websites. Additionally, web pages used to steal account credentials were disguised as Microsoft, Google, and Yahoo! login pages, hosted from web servers controlled by the attackers.

Authors of the Clearsky (2016) report underlined that cyberattacks by Molerats were considerably focused on targeting software developers. Illegitimate websites were poised to resemble legitimate sites for iOS applications. The attackers would try to lure software developers to this malicious website through online job postings.

DUSTYSKY, referred to as NeD by its developer, is a worm written in the Microsoft .NET Framework. DUSTYSKY would circumvent implanting itself in a running virtual machine (VM), and would extract itself only after having verified that it was not within the confines of a VM. After a system had been compromised, DUSTYSKY would determine the presence of an AV and gather data about the OS that it was running on. After these procedures had completed, a news document would be opened as a means of distraction, and the backdoor itself would be dropped onto the computer. DUSTYSKY would then begin data exfiltration by capturing screenshots and recording active processes running on the system, then sending them directly to their C2 infrastructure. It could also activate keylogging, find and spread itself to removable media or network storage, and turn off or restart the system. Additionally, attackers used the open-source tool BrowserPasswordDump to procure passwords within browsers (Clearsky, 2016).

Hypertext Transfer Protocol Secure (HTTPS) traffic was eventually phased into the C2 servers used in the DustySky attacks. This HTTPS traffic was signed by a legitimate digital certificate issued by the cybersecurity company Comodo (Clearsky, 2016). The use of this particular certificate could be related to the 2011 hacking of a digital certificate from Comodo by an Iranian cyber threat actor (ComodoHacker's Pastebin, n.d.).

Later that year, Clearsky (2016) published that Molerats had updated its TTPs within the DustySky operation, porting its malware to C++ and adding RAT tools such as POISONIVY, and NANOCORE to its arsenal. Authors published that the majority of attacks took place were in Israel, with smaller numbers in the US, several directed towards the Palestinian Authority, and 1% or less in a number of European and East Asian countries. They also underlined that, according to keywords requested by the malware regarding the files it sought to obtain, the

attackers were largely looking to acquire military intelligence regarding Israeli operations, databases, account information, login credentials, and information related to Bitcoin.

Discussion of the Findings

The purpose of this research was to study the capabilities of the cyber espionage operations undertaken by Iranian cyber threat actors. What is the methodology behind Iranian cyber attacks? What do the practices of Iranian cyber threat actors tell us about their strategy, structure, and purpose? What is the correlation between the TTPs utilized by Iranian cyber threat actors and those employed by Iran-linked groups outside the country?

Similarities in Attack Methodology

Iranian threat actors engaging in cyber espionage operations have evolved distinctly from one another, however, there are notable trends in their attack methodology, particularly their reliance on specific attack vectors to achieve initial compromise and their approach to exploiting legitimate services within a compromised system.

The two most common and longstanding identifiable features throughout the recorded history of Iranian cyber espionage operations are the use of professional or recruitment-themed spear phishing campaigns as a pretext to achieve initial compromise, and the leveraging of weaponized Microsoft Office documents with malicious macros as a means of delivering malware.

Many Iranian cyber espionage operations have involved at least partial use of a strategy known as "living off the land" when conducting lateral movement across compromised networks, privilege escalation against compromised systems, or data exfiltration. "Living off the land" strategy involves attackers exploiting legitimate tools and services within a compromised system in lieu of introducing malicious applications or software, which simplifies their

operations and reduces the risk of detection. This is exemplified by the Cleaver team's use of FTP - a legitimate network protocol - to exfiltrate data from compromised computers to the attacker's C2 infrastructure. It is also seen in the widespread exploitation of the Windows Sysinternals utility ProcDump by APT35, APT39, and the Cleaver team, as well as the exploitation of the Windows Credential Editor tool to escalate privileges within a compromised host, leveraged by APT39 and the Cleaver team. In addition, the employment of the Windows Sysinternals utility PsExec to achieve lateral movement throughout a network is exploited by APT33, APT34, APT35 and the Cleaver team.

Major Distinctions

Tactics, Techniques & Procedures (TTPs). It is important to not overstate the degree of resemblance between threat actors, as doing so may lead to misconceptions about appropriate defense measures, as well as false perceptions when discussing the relationship between Iranian cyber threat actors and structure of Iran's cyber nexus.

Publications by security vendors have acknowledged the occasional shared use of custom tools between threat actors, such as APT34 and APT39's dual implementation of the POWBAT backdoor (Hawley et al., 2019). Iranian threat actors also use publicly available tools, occasionally modifying or repurposing them to fit specific roles within their overlying attack strategy. Attackers employ a broad range of publicly available tools, but have, on occasion, maintained patterns in their use of specific ones. For instance, APT33, APT34, APT35, and APT39 and the attackers behind Operation Cleaver have all been observed using Mimikatz to perform either network pivoting, cached credential dumping, or privilege escalation. This broad range of functions is very relevant, as it suggests that the shared use of Mimikatz by multiple

cyber threat actors may not be the result of emulation or cooperation, but instead based on the wide number of circumstances in which Mimikatz tool can be applied.

Malware developed by Iranian cyber threat actors has ranged from relatively sophisticated to very simple. Cyberattacks waged by threat actors have utilized malware on both ends of this spectrum, sometimes in conjunction with one another. For instance, TINYZBOT, which was used throughout Operation Cleaver as a means of establishing persistence and conducting data exfiltration, was used in conjunction with JASUS, an ARP-poisoning tool that was underscored by analysts as having been below the standard of many publicly available tools made for the same purpose (Cylance, 2014). APT35 also exhibits this pattern, using the complex GHOLEE malware, which itself was a modified version of a high-end penetration testing tool by Core Impact, and the much more simplistic CWOOLGER keylogger (Pernet & Lu, 2015).

Despite employing such a range of custom-developed malware, there are very few instances in which Iranian cyber threat actors have shared the major strains of malware behind their operations. The notable exception to this is the shared use of the PowerShell backdoor POWRUNNER by APT34 and APT39. However, barring this instance, use of DROPSHOT and the subsequent TURNEDUP and SHAPESHIFT modules has been relegated to APT33, the HELMINTH backdoor to APT34, GHOLEE and the MAGICHOUND family of malware to APT35, TINYZBOT to the attackers behind Operation Cleaver, and the SEAWEED and CACHEMONEY backdoors to APT39.

Linguistic capabilities. One striking difference between Iranian cyber threat actors is their capability to leverage foreign languages into the context of their spear phishing campaigns. Social engineering often requires the use of language to create a convincing background with which to lull a target into a false sense of security, or to circumvent a real perception of danger.

The unconvincing or improper use of language is especially harmful to an attacker's efforts, as it may arouse suspicion regarding the pretext of the situation, and alert the target of an ulterior motive.

APT35 underwent significant evolutions in its extended history of cyber espionage operations, advancing the efficacy of its spear phishing and social engineering operations to more successfully achieve initial compromise. However, during the Thamar Reservoir campaign, believed to have dated back to mid-2014, their lack of convincing language skills caused considerable damage to their social engineering efforts, both in spoken vishing attacks and written spear phishing emails.

Contrarily, TEMP.Zagros was shown capable of leveraging multiple foreign languages – including Arabic, English, Georgian, Turkish and Tajik – within the context of its spear phishing campaigns (Lancaster, 2017). In these spear phishing campaigns, weaponized Microsoft Office documents used as a means of initial compromise resembled official government publications from agencies and organizations within the country of the respective target (Singh, et al., 2018). Though not explicitly outlined by any public reports, the ability of TEMP.Zagros to convincingly fabricate government publications speaks to their ability to effectively use formal and standardized modes of the aforementioned languages.

Operations security. During the Thamar Reservoir campaign, APT35 was revealed to have made enormous errors in the configuration of their C2 infrastructure. These configuration errors, which involved hosting publicly-facing web services without any login or password-based protection, allowed cybersecurity analysts direct access into the C2 infrastructure, to study APT35's activities. These findings also underscored that attackers from APT35 had infected their own machines with the campaign's malware, and thereby keylogged their own

communications, which were stored on the unsecured web servers. This collection of OPSEC grievances led to the discovery of a key attacker's identity, and opened a portal of understanding into the past and present workings of APT35 (Clearsky, 2015).

It is important to note that the intelligence report published by Clearsky (2015) indicated that the Thamar Reservoir campaign dated back to mid-2014, and that APT35 had been operating since between 2010 and 2011. This means that APT35's C2 infrastructure remained unsecured even as the group surpassed its fourth year of continuous cyber espionage campaigns.

Symantec's analysis of Leafminer also led to the discovery of an insecure C2 web server, which was accessible through a shell planted during the course of an attack. The subsequent research into Leafminer's operations led to the conclusion by analysts that attackers behind the one-year cyber espionage campaign were thwarted by their own inexperience, evident by their reliance on previously established vulnerabilities and poor implementation of OPSEC procedures (Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions, 2018).

Both APT35 and Leafminer stand out from other Iranian cyber threat actors as having significant OPSEC flaws in the security of their C2 infrastructure. But they also stand out from one another. APT35's vulnerable C2 infrastructure was discovered over four years into its cyber espionage operations, while Leafminer's C2 servers were uncovered when the group was estimated to have been only a year-and-a-half old. APT35 also had an exceptionally larger, more diversified list of cyber espionage campaigns under its belt, with custom malware and TTPs that displayed far more experience than Leafminer's singular operation.

Maturity. Emerging cyber threat actors, such as Leafminer and APT39, have demonstrated exceptionally different levels of maturity in their cyber espionage operations. Whereas Leafminer relied on the successful TTPs of other, more experienced cyber threat actors

across the whole of its operations, APT39 incorporated certain proven TTPs into its attack lifecycle alongside its own. For instance, Leafminer achieved initial compromise by mimicking the successful techniques of a known Russian APT, employed modified versions of publicly released cybersecurity tools to support its own operations, and incorporated evasive techniques discussed at a previous Black Hat EU conference to avoid detection. Leafminer's use of custom malware is limited, appearing twice as two modes of remote access, BACKDOOR.SORGU and TROJAN.IMECAB ("Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions", 2018).

Perhaps most importantly, Leafminer's internal workings were revealed after analysts at Symantec were able to enter their unsecured web server. On its own, the inability of the group to provide appropriate access control to their own C2 infrastructure was a key indicator of their inexperience. In this case, the blunder is even more significant because it marks the second time that a major Iranian threat actor has allowed a foreign cybersecurity firm to enter their C2 infrastructure due to an inherent lack of security configurations, the first time being against APT35 by Check Point Software Technologies (2015).

Meanwhile, although APT39's cyber espionage operations have strongly resembled those of APT34, it has nevertheless remained a distinct and separate APT. APT39 modified and carried over APT34's use of the POWBAT backdoor into its attack lifecycle, and has similarly-named C2 infrastructure. Both groups have also targeted several of the same major targets, but APT39 emerged with distinguishing characteristics of its own, such as an inherent focus on the targeting of the travel and telecommunications industries. It also employs custom suites of its own malware to achieve desired effects, such as the BLUETRIP, REDTRIP, and PINKTRIP tools that use SOCKS5 proxies to laterally move between compromised hosts, and the independent

CACHEMONEY and SEAWEED backdoors (Hawley et al., 2019). In comparison to Leafminer, APT39 has a much more extensive understanding of exploitation, going so far as to identify and exploit vulnerable web servers, then gather compromised credentials and use them to enter externally-facing Outlook resources. APT39 is also more proficient at leveraging a "living off the land" strategy against its targets.

The Question of Structure

The Iranian cyber nexus is obscured by the lack of knowledge concerning its structure, and a non-understanding of exactly which cyber threat actors are tied to one other, or how. Iranian threat actors are numerous, and this paper has not produced an exhaustive list of them. Instead, it has focused on the highest profile threat actors as a means of studying the apex of the Iranian cyber nexus. Singular threat actors within the Iranian cyber nexus may be independent hacktivist organizations, contractors to nation-state actors, or operators within the echelons of Iranian military organizations. Cybersecurity professionals throughout FireEye (2018), Cylance (2014) Check Point Software Technologies (2015), and Clearsky (2017) have all independently drawn links between individual threat actors conducting cyber espionage operations and the Iranian government, but the nature of these relationships is still unclear, largely due to the fact that the structure of the Iranian cyber nexus itself is so opaque.

The research conducted on Leafminer and APT39 has observed that, among two emerging cyber threats, one relies almost solely on emulating more experienced threat actors, and one has the propensity to apply lessons-learned concepts in such a way that augments their incoming cyberattacks. In other words, the maturity levels of Iran's emerging threat actors are explicitly divergent of one another. Additionally, Iranian threat actors develop their capabilities

at varying rates and in multiple directions, and there is a lack of congruity in the use of custom-developed malware.

These divergences all contradict the possibility that Iranian threat actors are being directly managed or developed in a rank-and-file manner. It could be the case that the structure of the Iranian cyber nexus is highly compartmentalized, wholly informal, or that different Iranian threat actors occupy different positions within the Iranian defense and intelligence sectors. But, regarding oversight, the details collected throughout this research are inconsistent with a singular, direct management structure.

This does not rule out the potential for some cyber threat actors to exist within the same command structures. Were different Iranian defense and intelligence organizations responsible for their own threat actors, it would explain the lack of congruity between individual groups, but also account for the notable instances where multiple groups, such as APT34 and APT39, appeared to either share resources or work together (Hawley et al., 2019).

The theory that Iranian cyber threat actors exist under separate command structures is further supported by the wide range of industries targeted by Iranian cyber espionage operations, which includes aerospace, defense, education, government, oil and gas, finance, media, technology, telecommunications, and transportation. The information gathered from these cyberattacks is far too broad to be believably utilized by a single entity. It is more plausible that Iranian cyber espionage operations exist separate from one another, each in support of their own strategic objectives by different political, military, and intelligence apparatuses within Iran.

An additional point of emphasis here is the understanding that data gathered by some Iranian cyber espionage operations is used to facilitate disruptive and destructive cyberattacks. This implies that some number of Iranian cyber espionage operations take place specifically to

support future cyberattacks, which is distinctly separate from cyber espionage as a form of strategic intelligence collection, and lends credence to the theory that these operations take place under separate command structures.

This theory on the use of separate command structures might contradict the Recorded Future report by Gundert, Chohan and Lesnewich (2018), in which they detailed the purported use of trusted middlemen to bid out taskings from the IRGC to private contractors. If that kind of fractured command structure were being leveraged throughout the Iranian cyber nexus, it would mean that the intelligence exfiltrated and gathered by Iranian threat actors was being received by the same overarching entity. Still, it could be the case that different hierarchies within the IRGC, which is very broad and extensive organization, are responsible for ordering these taskings. If that were true, it would mean that separate command structures did exist as taskings traveled back and forth from IRGC officials to the respective contractor organizations. However, no evidence has been published to support this notion.

Perhaps the strongest evidence that Iranian cyber espionage operations take place under different command structures lies in the Telegram channel Lab Dookhtegan, which claimed that the Iranian Ministry of Intelligence and APT34 were the same entity, publishing tools used by APT34 as well as the alleged identities and personal information of the attackers. This finding separates the pinnacle of the cyber nexus between the frequently-referenced IRGC and the Iranian Ministry of Intelligence, identifying two distinct entities at the forefront of Iranian cyber espionage operations. It also backs up the statement by Anderson and Sadjadpour (2018) that both the IRGC and the Ministry of Intelligence conduct their own offensive cyber operations.

Lab Dookhtegan and Iran's Insider Threat

The existence of Lab Dookhtegan also raises significant questions about cyber espionage internal to Iran. If the users behind Lab Dookhtegan are, as they appear to be, domestic attackers working against the Iranian government, then that would carry new implications on the cyber ecosystem of Iran. Details within the Lab Dookhtegan Telegram channel support this, especially the native quality of the Farsi written in their messages alongside the imperfect English translations, however it should be noted that these conditions could be fabricated.

Distinctions Between Iranian and Lebanese Threat Actors

When this paper sought to establish a connection between the TTPs utilized by Iranian cyber threat actors and those of the Iran-linked groups outside the country, there was an understanding that such a connection may be indicative of cyberspace-based cooperation between Iran and its regional allies. Part of this had been prefaced by the longstanding alliance between Iran and Lebanese Hezbollah, which began with the Iranian aggregation and organization of Lebanese Hezbollah during the 1982 Lebanon War with Israel. Since this inception, Lebanese Hezbollah has been a partner to the Iranian regime, working together to conduct intelligence and wage military operations against foreign adversaries of the Iranian regime (Levitt, 2015). So, in 2015, when the Volatile Cedar campaign became attributed to Lebanese Hezbollah in the midst of rising Iranian cyberattacks, it called into question whether the political and military relationship between both entities had expanded into the cyberspace domain.

Despite that historical background, this paper found that the TTPs of the Volatile Cedar campaign by Lebanese Hezbollah were fundamentally different from any of the recorded cyberattacks by major Iranian threat actors. That difference extends to Dark Caracal, the threat

actor attributed to the Lebanese intelligence agency GDGS. The distinctiveness of each individual set of TTPs suggests that they were not influenced or developed with the help of one another. This does not negate the similarities in target selection and broader strategy between Iranian and Lebanese Hezbollah cyber threat actors, however, there are no indications of shared resources within the attack frameworks of these parties. In this way, there is a lack of evidence to purport that Iranian cyber threat actors have contributed to the cyber espionage capabilities of Lebanese Hezbollah.

Lebanese Hezbollah. Analysis of the Volatile Cedar campaign found no correlation between the TTPs of Lebanese Hezbollah's cyber espionage operations and those of Iranian cyber threat actors. Cyberattacks conducted throughout Volatile Cedar targeted public-facing web servers directly, and did not incorporate social engineering into their compromise of computer systems (Check Point Technologies, 2015). This starkly contrasts the TTPs of major Iranian threat actors, which have traditionally involved extensive spear phishing campaigns and other social engineering efforts to distribute malware onto a target host. Volatile Cedar's use of web servers as an entry point into the internal networks of an organization are also distinct from the strategies employed by Iranian counterparts.

The EXPLOSIVE malware leveraged by the Volatile Cedar campaign was unique in its use of custom encoding algorithms to evade detection. The strategic use of EXPLOSIVE also stood out from Iranian cyber espionage operations; whereas Iranian threat actors often relied on an array of custom-developed and publicly available malware to conduct a cyberattack in separate stages, Volatile Cedar's operations primarily revolved around EXPLOSIVE, relying on its multi-faceted capabilities to administer all phases of their cyberattacks after initial compromise had taken place (Check Point Technologies, 2015).

Dark Caracal. Research into the cyber espionage operations run by Dark Caracal revealed a wholly different cyber threat than any posed by Iranian threat actors, or by Lebanese Hezbollah. Dark Caracal's operations differentiated from others with a strong focus on mobile-based cyberattacks, embedding the PALLAS malware into malicious versions of popular chat applications, and leveraging different social engineering attacks to con users into installing the malicious applications (Blaich, et al., 2018). No evidence was found correlating the TTPs of Dark Caracal to any Iranian APT, nor to the cyber espionage operations by Lebanese Hezbollah.

Connections Between Iranian and Palestinian Threat Actors

Palestinian cyber espionage operations have left a significantly smaller imprint than their Iranian and Lebanese counterparts. Although TTPs utilized by Molerats bore some shared characteristics with those of Iranian threat actors, the stark differences in the competence with which these TTPs were carried out calls into question whether any similarities are intentional or simply coincidental. For instance, both Iranian and Palestinian cyber threat actors employed spear phishing tactics utilizing multilingual, professionally-geared email attachments to establish initial compromise (Clearsky, 2016). But spear phishing emails from the Palestinian-linked Molerats group were made with of a significantly lower quality than those created within the context of Iranian cyber espionage operations, and did not mimic the techniques in Iranian spear phishing campaigns in such a way that would suggest direct influence.

The use of the RAT NANOCORE by both Molerats and APT33 is another faint link here, but NANOCORE is publicly available and not custom designed either by Iranian or Palestinian actors, and the use of publicly available malware by Molerats is repeated in its leveraging of POISONIVY, which had originally been associated with Chinese cyberattacks (Clearsky, 2016).

However, one visible connection between Iranian and Palestinian cyber espionage operations is Molerats' use of a legitimate digital certificate – published by Comodo – to sign C2-based HTTPS traffic. The use of this digital certificate is a noteworthy, as it correlates to the 2011 theft of a digital certificate from Comodo (ComodoHacker's Pastebin, n.d.). Within a five-year period, this digital certificate was allegedly stolen by a single Iranian attacker, and resurfaced as a resource to a cyberattack perpetrated by Palestinian threat actors.

Future Research

What is Strategic Intelligence Acquired by Iranian Cyber Espionage Being Used For?

The chronology and analysis of Iranian cyber espionage operations in this paper all lead into the question of purpose. Iranian cyber threat actors do not target indiscriminately, they focus their efforts on exfiltrating information from specific organizations within key industries, nearly all of which belong to one of several countries, in particular the KSA, Israel, and the US. This target range encompasses a wide spectrum of industries, including aerospace, defense, education, government, oil and gas, technology, telecommunications, and transportation. What this means is that the strategic intelligence extracted from Iranian cyber espionage has a large range of applications, including use in military intelligence, industrial espionage, political sabotage, and influence operations. Therefore, it is likely that this strategic intelligence is being used to support multiple objectives, perhaps by entirely different organizations and agencies within the Iran.

This inquiry is strongly connected to the question of Iranian cyber nexus structure, which, as aforementioned, is highly obscured and difficult to surmise. However, while research into the TTPs of Iranian threat actors sheds light on how they conduct cyber espionage operations, further analysis into the post-exfiltration activities of the same Iranian threat actors would allow

cybersecurity professionals discern where the information collected by Iranian cyber espionage operations is eventually forwarded to, and thereby discern what it is being used for.

What Role Do Less Prominent Cyber Threat Actors Play In The Iranian Cyber Strategy?

The Iranian threat actors discussed within this research are the most publicly discussed and documented of their ilk, but the list is far from exhaustive. As aforementioned, Iranian cyber threat actors, both APTs, secondary groups, and individuals, all appear and reappear under various names and aliases, which makes it difficult to identify structures among Iranian cyber threat actors and their regional allies, and to connect their activities to one another. Incidentally, several Iranian and Iran-linked cyber threat actors exist outside of this

In an exclusive interview with Flashpoint, the Iranian cyber threat actor Parastoo, a self-defined "cyber movement," alluded to connections with a large conglomerate of other groups, including Emad Brigades, Bosnian Cyber Army, Karbala Electronic Warfare, Idnol'Jihad, Iranian Cyber Army, Islamic Resistance Group, Syrian Electronic Army, Mansooroon and Sobh Cyber Jihad (Inside an Iranian Hacker Collective: An Exclusive Flashpoint Interview with Parastoo, 2016). It is difficult to determine whether these groups and others like them are sharing resources at some level, working in mutual pursuit of a specific objective, or supporting the broader strategy of the Iranian nation-state. There also exists the potential for these groups to be part of a larger, politically-oriented hacktivist activity, directing cyberattacks at international opponents of the Iran and its allies.

Oftentimes the cyberattacks waged by these lesser-known threat actors are not as sophisticated than those of the more prominent cyber threat actors discussed in this paper. Regardless, their presence in the landscape of cyberspace is noteworthy, at first because it is unclear what their role is in relation to the Iranian nation-state itself, but also due to each group's

potential to evolve into a more advance threat. For these reasons, understanding the larger conglomerate of Iran-linked cyber threat actors is necessary in defining the broader capabilities of Iranian cyber power.

How is Cyber Espionage Leveraged Internally Against the Iranian Populace?

The research conducted within this paper concerns the application of cyber espionage operations against international targets, but does not address the use of cyber espionage within Iran itself. As Anderson and Sadjadpour (2018) have published, cyber threat actors inside Iran have and continue to employ cyber espionage against Iranian government officials, reformist politicians, members of the media, religious and ethnic minorities, major cultural figures, and various insurgent and separatist movements. The methodology by which these cyber espionage activities take place varies from sophisticated cyberattacks to persistent attempts at account compromise.

The use of cyber espionage within Iran raises an abundance of questions regarding who the threat actors are and what purpose the information gained through their domestic cyberattacks serves. For instance, do these domestic cyber espionage operations produce actionable intelligence, and if so, how are they further acted upon? Additionally, what organizations throughout Iran have the authority to conduct these domestic cyberattacks? What systems are already in place to allow for the monitoring of digital communications within Iran?

Answers to these and other questions stemming from the initial one would assist cybersecurity professionals in understanding domestic cyber surveillance through a different lens, including the abuse of these powers by state-based institutions. It would also allow for comparative research to measure similarities and differences between the different applications

of Iranian cyber espionage, and to discern whether or not correlations exist between cyberattacks pointed at external targets and those against internal ones.

Recommendations

When FireEye (2018) published its annual trend report detailing Iranian cyber espionage operations, it underscored that the character of Iran-linked cyber threat actors had grown from petty hacktivist activity to sophisticated APTs. As a collective of major cybersecurity vendors all track and report the increased aggression and complexity of these operations, Iran becomes more relevant in discussing about the future of international conflict and the use of non-traditional mediums in which it may take place.

This is not a doomsday prophecy, it is an observation of a nation-state actor developing its offensive cyberspace capabilities in a relatively short time period, largely unimpaired by technological, budgetary, and manpower constraints that would otherwise impede it. Such capabilities create a menace out of actors that may otherwise be unable to contend with larger, more advanced powers. In this equation, cyber espionage augments intelligence collection to perform at a capacity that would be difficult to attain without the exploitation of digital networks, in such a way that traditional intelligence practices are incapable of keeping up with.

There is no be all, end all solution to the problems posed here. Iranian cyber threat actors have capitalized on the use of people – the weakest point in any organization's security posture – as an entry point into digital networks. Many have demonstrated the ability to develop customized attacks pertinent to specific targets, adapt their TTPs to compromise new and emerging technologies, and apply lessons-learned concepts to their future operations. The various industries and sectors targeted by these operations are massive in scope, and put a large, international conglomerate of governments, corporations, organizations and institutions at direct

risk of attack. To mitigate this risk, cybersecurity professionals will need to consider the TTPs of Iranian cyber threat actors alongside the velocity of their cyber espionage operations, in order to counter the technological threats presented, and to defend their assets with the same persistence that the adversary maintains to attack them.

References

Anderson, C., & Sadjadpour, K. (2018). *Iran's cyber threat*. Washington DC: Carnegie Endowment for International Peace.

Blaich, A., Kumar, A., Richards, J., Flossman, M., Quintin, C., Galperin, E. (2018). *Dark Caracal: Cyber-espionage at a Global Scale*. Retrieved January 31, 2019.

Cilluffo, F. (2012). *The Iranian Cyber Threat to the United States*. Washington DC: George Washington University. Retrieved from https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-071c.pdf

Cilluffo, F. (2016). *Emerging Cyber Threats to the United States*. Washington DC: George Washington University. Retrieved from https://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-Wstate-CilluffoF-20160225.pdf

Check Point Software Technologies. (2015). *Rocket Kitten*. Check Point Software Technologies. Retrieved from https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

Check Point Software Technologies. (2015). *Volatile Cedar*. Check Point Software Technologies.

Clearsky. (2015). *Thamar Reservoir*. Clearsky. Retrieved from https://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public.pdf

ClearSky. (2016). Operation DustySky. Retrieved January 31, 2019.

ClearSky. (2016). Operation DustySky - Part 2. Retrieved January 31, 2019.

ComodoHacker's Pastebin. Pastebin.com. Retrieved from https://pastebin.com/u/ComodoHacker

Cylance. (2014). *Operation Cleaver*. Cylance Inc. Retrieved from https://www.cylance.com/content/dam/cylance/pages/operationcleaver/Cylance_Operation_Cleaver_Report.pdf

Eisenstadt, M. (2016). *Iran's lengthening cyber shadow*. Washington, DC: The Washington Institute for Near East Policy.

Falcone, R. & Lee, B. (2016). The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor [Blog]. Retrieved from https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

FireEye (2018). *M-Trends 2018*. Milpitas: FireEye, Inc. Retrieved from https://investors.fireeye.com/static-files/b7dcb16f-44a8-4cfb-927f-efeed397dd52

FireEye (2019). *M-Trends 2019*. Milpitas: FireEye, Inc.. Retrieved from https://content.fireeye.com/m-trends

Fixler, A., & Cilluffo, F. (2018). *Evolving menace: Iran's use of cyber-enabled economic warfare.* Foundation for Defense of Democracies. Retrieved from https://www.fdd.org/wp-content/uploads/2018/11/REPORT_IranCEEW.pdf

Gholee. (2014). [Blog]. Retrieved from https://www.clearskysec.com/gholee-a-protective-edge-themed-spear-phishing-campaign/

Grunzweig, J. & Falcone, R. (2016). OilRig Malware Campaign Updates Toolset and Expands Targets [Blog]. Retrieved from https://unit42.paloaltonetworks.com/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/

Gundert, L., Chohan, S. and Lesnewich, G. (2018). *Iran's Hacker Hierarchy Exposed*. [online] Recorded Future. Available at: https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf [Accessed 19 Apr. 2018].

Hawley, S., Read, B., Brafman-Kittner, C., Fraser, N., Thompson, A., Rozhansky, Y., Yashar, S. (2019). APT39: An Iranian Cyber Espionage Group Focused on Personal Information [Blog]. Retrieved from https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html

Healey, J. (2013). *A fierce domain* (p. 229). Vienna, Va.: CCSA.

Inside an Iranian Hacker Collective: An Exclusive Flashpoint Interview with Parastoo. (2016). Retrieved from https://www.flashpoint-intel.com/blog/cybercrime/inside-an-iranian-hacker-collective-an-exclusive-flashpoint-interview-with-parastoo/

Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford. (2018). [Blog]. Retrieved from https://www.clearskysec.com/oilrig/

iSight Partners Inc., (2014). *Newscaster*. iSight Partners Inc. Retrieved from https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/2014.05.28.NewsCaster_An_Iranian_Threat_Within_Social_Networks/file-2581720763-pdf.pdf

Lancaster, T. (2017). Muddying the Water: Targeted Attacks in the Middle East. Retrieved March 15, 2018.

Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions. (2018). [Blog]. Retrieved from https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east

Lee, B. & Falcone, R. (2017). Magic Hound Campaign Attacks Saudi Targets. Retrieved December 27, 2019.

Lee, B. & Falcone, R. (2018). OilRig Targets Technology Service Provider and Government Agency with QUADAGENT [Blog]. https://unit42.paloaltonetworks.com/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/

Lee, B. & Falcone, R. (2018). OopsIE! OilRig Uses ThreeDollars to Deliver New Trojan [Blog]. Retrieved from https://unit42.paloaltonetworks.com/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/

Levitt, M. (2015). *Hezbollah.* Washington: Georgetown University Press.

Morell, M., & Harlow, B. (2015). *The great war of our time*. New York: Twelve.

Mundo, A., Roccia, T., Saavedra-Morales, J., & Beek, C. (2018). Shamoon Returns to Wipe Systems in Middle East, Europe [Blog]. Retrieved from https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-returns-to-wipe systems-in-middle-east-europe/

Nasr, S. (2006). *The Shia revival*

Sardiwal, M., Cannon, V., Fraser, N., Londhe, Y., Richard, N., O'Leary, J. (2017). *New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit*. Retrieved from https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

Singh, S. & Chang, Y. (2016). Targeted Attacks against Banks in the Middle East [Blog]. Retrieved from https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html

Singh, S., Jallepalli, D., Londhe, Y., & Read, B. (2018). Iranian Threat Group Updates Tactics, Techniques and Procedures in Spear Phishing Campaign [Blog]. Retrieved from

https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html

Suspected Hacker Group Creates Network of Fake LinkedIn Profiles. (2015). Retrieved from https://www.secureworks.com/research/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles

The Cyber Party of God. (2018). Retrieved from http://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/

O'Leary, J., Kimble, J., Vanderlee, K., & Fraser, N. (2017). *Insights into Iranian cyber espionage: APT33 targets aerospace and energy sectors and has ties to destructive malware*. Retrieved from https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

Pernet, C., & Lu, K. (2015). *Operation Woolen Goldfish*. Irving: Trend Micro, Incorporated. Retrieved from https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-woolen-goldfish.pdf

Pernet, C., & Sela, E. (2015). *The spy kittens are back*. Trend Micro, Incorporated. Retrieved from https://documents.trendmicro.com/assets/wp/wp-the-spy-kittens-are-back.pdf

The Curious Case of Mia Ash. (2017). Retrieved from https://www.secureworks.com/research/the-curious-case-of-mia-ash

Villaneuva, M., Co, M. (2018). Another Potential MuddyWater Campaign uses Powershell-based PRB-Backdoor [Blog]. Retrieved from https://blog.trendmicro.com/trendlabs-security-intelligence/another-potential-muddywater-campaign-uses-powershell-based-prb-backdoor/

Villeneuve, N., Moran, N., Haq, T., & Scott, M. (2013). *Operation Saffron Rose*. FireEye. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf

Villeneuve, N. (2013). Operation Molerats: Middle East Cyber Attacks Using Poison Ivy [Blog]. Retrieved from https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html