Cyberint

Iranian Cyber Capabilities & Threats

January 2020

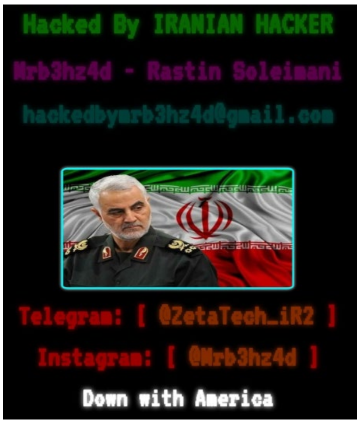
Table of Contents

Executive Summary

Following the US Military announced assassination of the Iranian General Qassem Suleimani, leader of the Iranian Islamic Revolutionary Guard Corps (IGRC) Quds force, on 3 January 2020, there is heightened threat of reprisal from the Iranian government and pro-Iranian groups against targets in both the United States and their allies.

Whilst there was an initial military response with missiles being launched at US coalition bases in Iraq on January 7, the allegedly accidental downing of Ukraine International Airlines flight PS752 appears to have tempered the appetite for further physical attacks.

Throughout these developments, low sophistication cyber-attacks were observed, such as website defacements conveying politically motivated pro-Iranian and anti-American sentiments (Figure 1), although these were likely conducted by individuals or disorganized threat groups rather than being orchestrated by the Iranian state.



Hacked By IRANIAN HACKER

Mrb3hz4d - Rastin Soleimani

hackedbymrb3hz4d@gmail.com

Telegram: [@ZetaTech_iR2]

Instagram: [@Mrb3hz4d]

Down with America

Figure 1 – Website defacement (Source: https://mobile.twitter.com/kbrackson/status/1213334433807265793)

Given Iran's known cyber offensive capabilities, the media have been speculating of the potential for cyberattacks in response to the escalating incident, especially threat against critical infrastructure. Although there is no evidence of Iranian nation-state sponsored cyber-attacks in retaliation for Suleimani's death, especially against the US, Israel and their allies, organizations should familiarize themselves with past Iranian-nexus tactics, techniques and procedures (TTP) to better protect themselves from any apparent risk.

This report provides an overview of ten suspected Iranian nation-state sponsored threat groups, referenced by their MITRE ATT&CK™ identifiers, along with their common TTP.

Without causing undue alarm, organizations previously targeted by Iran, such as government, military and critical national infrastructure targets in the US and ally nations along with the regional petrochemical industry and organizations located in rival nations, will likely continue to be targeted. Past Iranian cyber activity suggests that watering hole attacks could be utilized in new cyber offensives and therefore there is potential for the targeting and compromise of organizations in other industries, such as seen with newspaper websites being compromised by the Iranian group known as 'CopyKittens', although this could be considered collateral damage. Furthermore, Iranian threat groups have been known to target supply chains and as such, those interacting and dealing with 'legitimate' targets will be at increased risk, for example, the defense industry as well as technology providers.

Consistent TTP for Iranian-nexus threat groups includes the delivery of spear phishing emails, repeatedly using job vacancy lures, as well as the exploitation of common vulnerabilities and the delivery of both custom and readily available malicious payloads. As such, and in accordance with the threat landscape as a whole, organizations should seek to eliminate these oft-used attack vectors by educating their users and practicing good cyber hygiene by ensuring systems are patched regularly. Additionally, users, especially high-risk individuals, should be cautious of social media interactions with unknown and untrusted parties as Iranian threat groups have been known to attempt to conduct social engineering and disinformation campaigns via common social media platforms.

Background

Following the recent developments in the middle East, including the assassination of Iranian General Qassem Suleimani, leader of the Iranian QUDS force, on Friday 3 January 2020, there has been heightened threat of reprisal from the Iranian government and pro-Iranian groups against targets in both the United States and their allies.

Covert action such as launching cyber-attacks will undoubtedly be a compelling option for Iran, especially given past-activity and their expertise in this theatre.

Although speculation of potential cyber targets includes the obvious, namely US government, military and critical national infrastructure establishments, pro-Iranian website defacements have indiscriminately targeted organizations whilst intelligence-gathering and disruption activities could be directed at any industry. Furthermore, attacks against the more obvious targets could commence with third-party and supply-chain compromises and as such, those dealing with the US government, military or critical national infrastructure should be cautious.

Developments following the downing of flight PS752, Iranian disinformation campaigns are likely to be pushed via social media in an attempt to influence the media through fake news, alternate narratives or simply the creation of new headlines, such as the compromise of a major brand or other attention-grabbing incident to divert attention away from investigation into the true cause of the crash. Furthermore, organizations should be aware of the potential for attack lures to be based on news or topics related to the conflict and flight PS752, such as seen in cyber activity following the downing of Malaysian Air flight MH17 over Ukraine in 2014.

Those with a physical presence in the region will no doubt be bolstering their physical security arrangements and organizations worldwide should familiarize themselves with past Iranian nation-state cyber activity to understand any potential risk and adequately prepare themselves for any potential fallout, be that direct attacks or collateral damage from broader anti-US campaigns.

Finally, it should be noted that whilst Iran are the current 'big' topic, other cyber threats will continue to exist and should not be forgotten. It is important to understand the realistic threats from Iran and factor these risks into an overall security strategy compared to other threat actors. Although some may be legitimate targets and are right to be alarmed, many organizations can settle for increased vigilance and common-sense to protect themselves.

Iranian Nation-State Sponsored Threat Groups

Various cybersecurity organizations and vendors have been tracking potential nation-state sponsored and advanced persistent threat (APT) groups believed to be affiliated with and/or aligned to Iranian state interests for many years. Given the complexity in attribution and the undoubted overlap in operations conducted by threat groups, many vendors and organizations assign their own codenames and monikers which can lead to some crossover and potential confusion. For the purpose of this Iranian cyber capabilities report, suspected Iranian threat groups have be classified by their MITRE ATT&CK™ Group identifier (Gxxxx) and known or suspected synonyms and associations referenced.

Furthermore, any observed tactics, techniques and procedures (TTP) have been aligned with the corresponding MITRE ATT&CK™ Technique (Txxxx) descriptions whilst the malware and tools utilized are aligned with MITRE ATT&CK™ Software (Sxxxx) profiles.

In addition to allowing each element to be easily cross-referenced using industry-standard identifiers, the use of MITRE ATT&CK™ allows defenders to determine how they can protect, detect and contain these threats.

For further information, each MITRE ATT&CK™ reference can be viewed on MITRE's website by replacing 'xxxx' with the relevant identifier within the appropriate URLs below:

Groups:	https://attack.mitre.org/groups/G*xxxx*;
Tools:	https://attack.mitre.org/groups/T*xxxx*;
Software:	https://attack.mitre.org/groups/S*xxxx*;

APT33 (G0064)

Active since at least 2013 and also known as 'Elfin' (Symantec[1]), 'Holmium' (Microsoft[2]), 'Magnallium' (Dragos[3]) and 'Refined Kitten' (Crowdstrike), APT33 (Fireeye[4]) is a suspected Iranian threat group that has previously targeted organizations in Saudi Arabia, South Korea and the United States with an apparent focus on the Aerospace and Energy industries.

Based on APT33's observed activities, the following MITRE ATT&CK™ Techniques have been identified (Figure 2).

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Spearphishing Link	Exploitation for Client Execution	Registry Run Keys / Startup Folder	Exploitation for Privilege Escalation	Execution Guardrails	Brute Force
Valid Accounts	PowerShell	Scheduled Task	Scheduled Task	Obfuscated Files or Information	Credential Dumping
	Scheduled Task	Valid Accounts	Valid Accounts	Valid Accounts	Network Sniffing
	User Execution				

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Network Sniffing	Remote File Copy		Commonly Used Port	Data Compressed	
			Data Encoding	Exfiltration Over Alternative Protocol	
			Remote File Copy		
			Standard Application Layer Protocol		
			Standard Cryptographic Protocol		
			Uncommonly Used Port		

Figure 2 – APT33 (G0064) – Identified MITRE ATT&CK™ Techniques

Notable Campaign: Aerospace & Energy Industry Employees Targeted by Fake Job Ads

Observed during 2016 and 2017, APT33 was targeting organizations based in South Korea and the United States, operating within the aerospace and energy industries, with commercial ties to Saudi Arabian organizations. These cyberespionage campaigns appeared to have be used to gain intelligence on Saudi

[1] https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

[2] https://www.wired.com/story/iran-apt33-industrial-control-systems/

[3] https://dragos.com/resource/magnallium/

[4] https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

Arabia's military aviation and petrochemical operations likely in an attempt to further Iran's military capabilities and their own petrochemical industry.

In these campaigns, APT33 has repeatedly been observed as sending spear phishing emails (T1192) masquerading as recruitment and employment opportunities to employees at aviation organizations with malicious HTML application (HTA) file attachments. If executed by the user (T1204), the HTA file displayed a decoy job description or vacancy, harvested from a legitimate posting, whilst downloading a malicious backdoor component. In similar themed campaigns, weaponized RAR archives have also been delivered to potential victims, again masquerading as files containing details of a job vacancy, in an attempt to exploit CVE-2018-20250[5], a path traversal vulnerability in WinRAR, and subsequently attempting the installation of additional components.

APT33 has repeatedly utilized domain masquerading in the spear phishing and payload download phases of their attack typically using dynamic DNS (DDNS) services with subdomains that mimic the target organization's domains or the domains of their partners or suppliers. Of the DDNS domain observed, it appears as though APT33 have a preference for using DDNS domains owned by the 'No-IP' service, including 'ddns.net', 'myftp.org', 'servehttp.com' and 'sytes.net', although it would presumably be trivial for them to switch to utilizing other providers.

Notably, these behaviors continued through 2018 with CyberInt Researchers identifying the very same TTP being used in targeted attacks against multiple organizations operating in the Saudi Arabian petrochemical industry[6].

APT33 has utilized numerous tools throughout their campaigns including custom backdoors such as 'Powerton' (S0371) and 'StoneDrill' (S0380), the latter of which includes destructive disk wiping capabilities, as well as backdoors created using the legitimate automation tool 'AutoIt' (S0129). Additionally, the group have utilized commodity malware including backdoors and remote access tools (RAT) such as 'DarkComet' (S0334) and 'NanoCore' (S0336).

Following the deployment of the backdoor component, be that custom or commodity, multiple persistence methods have been observed including adding files to the victim's Windows startup folder (T1060) as well as the creation of scheduled tasks (T1053) to ensure the backdoor continues to run.

Subsequently, in addition to information stealing capabilities, credential dumping (T1003) takes place using either features within the backdoor itself, such as network sniffing (T1040) capabilities used to gather

[5] https://nvd.nist.gov/vuln/detail/CVE-2018-20250

[6] https://blog.cyberint.com/bad-job-apt-fake-vacancy-campaign-targeting-saudi-arabian-petro-chemical-industry

credentials directly from network traffic, or through the use of publicly available tools such as ‘Mimikatz’ (S0002).

Recommendations

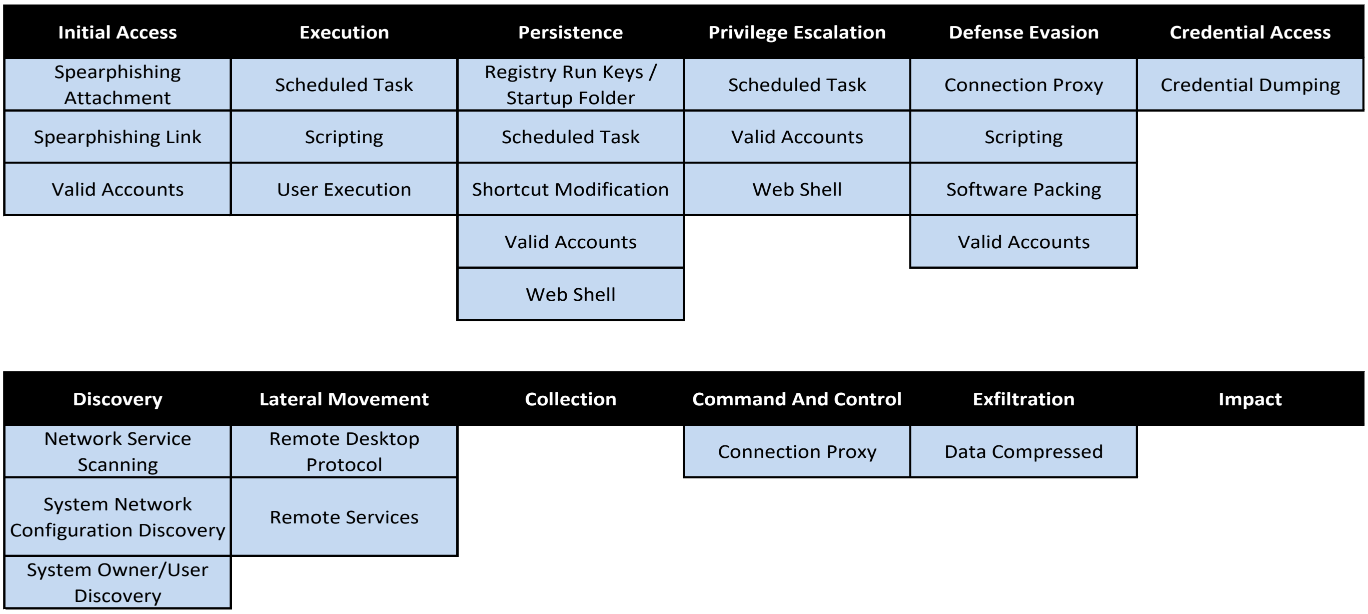
In addition to understanding and taking steps to mitigate any identified APT33 ATT&CK techniques that are considered critical within an organization’s environment, the following key elements should be considered:

- Suspicious file types, such as HTML Applications (HTA) used in APT33’s campaigns, should be rejected or quarantined by email gateways to prevent delivery to end-users
- Archive files, such as the weaponized RAR files sent as email attachments, should also have their content scanned or reviewed and those containing suspicious file types such as scripts or executables should be rejected or quarantined
- Dynamic DNS (DDNS) hosts, except those explicitly used and approved by the organization, should be blocked, and access attempts monitored, to prevent malicious payloads being downloaded from untrusted sources and to identify communication attempts with malicious infrastructure

APT39 (G0087)

Active since at least 2014 and aligning with the activities of a group known as 'Chafer' (Symantec[7]), APT39 (Fireeye[8]) is an Iranian threat group focused on stealing personal identifiable information (PII) from targets in the IT, telecommunications and travel industries across the Middle-East as well as France and the United States. Based on reports on APT39 activity thus far, it is believed that the targets of this PII theft are likely persons of interest to the Iranian state and data is gathered to facilitate the tracking and surveillance of these individuals. Additionally, it is suggested that data gathered during these operations may provide intelligence for APT39, or other Iranian nation-state sponsored threat groups, that can be leveraged in other campaigns.

Based on APT39's observed activities, the following MITRE ATT&CK™ Techniques have been identified



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Spearphishing Attachment	Scheduled Task	Registry Run Keys / Startup Folder	Scheduled Task	Connection Proxy	Credential Dumping
Spearphishing Link	Scripting	Scheduled Task	Valid Accounts	Scripting	
Valid Accounts	User Execution	Shortcut Modification	Web Shell	Software Packing	
		Valid Accounts		Valid Accounts	
		Web Shell			

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Network Service Scanning	Remote Desktop Protocol		Connection Proxy	Data Compressed	
System Network Configuration Discovery	Remote Services				
System Owner/User Discovery					

Figure 3 – APT39 (G0087) – Identified MITRE ATT&CK™ Techniques

Notable Campaign: Telecoms & Travel Targeted

Observed during December 2018, APT39 utilized TTPs similar to other Iranian nexus campaigns to target organizations in the telecommunications and travel industries with the objective of stealing personal data. Although organizations in France and the United States were targeted, the majority of observed activity appeared to focus on Middle Eastern targets including surveillance operations against domestic individuals and those 'closer to home'. In addition to gathering personal identifiable information (PII) from the target

[7] https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

[8] https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html

organizations, it is also suggested that commercial sensitive data may have also been collected, be that to benefit Iranian state interests or simply an intelligence gathering exercise to gain leverage in other campaigns.

APT39 was observed as sending spear phishing emails with malicious attachments (T1193) and/or links (T1192) to deliver backdoor payloads. As seen in other Iranian nexus campaigns, APT39 also utilized masquerade domains to appear legitimate and familiar to potential victims when opening lures as well as appearing inconspicuous to network or security monitoring. In addition to sending lures to victims, APT39 also conducted compromise operations including the exploitation of vulnerable web servers to install web shells (T1100) such as 'ASPXSpy' (S0073), typically allowing full access to the underlying operating system of the compromised host, as well as abusing stolen credentials to gain access to webmail services.

Following the initial compromised, APT39 has deployed custom backdoors, including 'CacheMoney' and 'Seaweed', as well as a variant of 'POWBAT', to establish a foothold and subsequently attempt to elevate their privileges through the use of credential dumping tools such as 'Mimikatz' (S0002) and the legitimate 'Windows Credential Editor' (S0005).

Having escalated their privileges or gained access to credentials, APT39 conducted network reconnaissance through port scanning (T1046) using a custom tool known as 'BLUETORCH' as well as native networking tools such as 'nbtscan' (T1016). Subsequently, the group continue to use legitimate and native tools, somewhat 'living off the land', and move laterally across the victim network using tools and techniques such as 'PsExec' (S0029) as well as remote services (T1021) including SSH and the Remote Desktop Protocol (RDP) (T1076).

Finally, having located and gathered the required PII, APT39 makes use of compression utilities, such as 7-Zip and WinRAR, to compress the data ready for exfiltration (T1002).

Recommendations

In addition to understanding and taking steps to mitigate any identified APT39 ATT&CK techniques that are considered critical within an organization's environment, the following key elements should be considered:

- Suspicious email attachments should subject to review or quarantine to prevent them from being delivered to unsuspecting end-users
- Masquerade domains typically utilize newly registered domain names or dynamic DNS (DDNS) hosts and as such, we recommend preventing access to newly registered domains with little-to-no reputational and unrecognized DDNS hosts
- Standard user accounts should not be permitted to execute native tools and utilities, such as those used for network or system administration, to prevent their misuse in the event of an account compromise
- Inspection of outbound network traffic may identify data loss scenarios such as the transmission of illegitimate archive files containing data for exfiltration, especially those using compression and/or encryption methods that are atypical for the organization.

Charming Kitten (G0058)

Active since at approximately 2014, ‘Charming Kitten’ (ClearSky Cyber Security[9]) is an Iranian cyberespionage group that has previously targeted persons of interest to the Iranian state, specifically those working in academic research and human rights as well as the media both domestically within Iran as well as individuals from Israel, the United Kingdom and the United States. Whilst the TTP of this group overlap with ‘Magic Hound’, another Iranian threat group, their operations appear to be conducted by separate groups.

Based on Charming Kitten’s observed activities, the following MITRE ATT&CK™ Techniques have been identified (Figure 4).

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
	Command-Line Interface	Registry Run Keys / Startup Folder			
	PowerShell				
	User Execution				

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Query Registry			Standard Application Layer Protocol		
System Information Discovery					
System Owner/User Discovery					

Figure 4 – Charming Kitten (G0058) – Identified MITRE ATT&CK™ Techniques

Typical Campaign: Persons of Interest Targeted

Rather than detailing a notable campaign, especially given that Charming Kitten focuses on targeting individuals, it is better to gain an understanding of Charming Kitten’s modus operandi and their typical campaign characteristics.

Given the nature of the target, an individual rather than an organization, Charming Kitten has attempted to compromise both private email accounts as well as any social media presence to gain access to personal communications as well as relationships and dealing with others. Whilst it may be advantageous to gain access to the victim’s devices, this is reported as being a secondary objective, likely due to increasing the chances of detection versus the remote monitoring of online services.

[9] https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf

Similar to other Iranian nexus campaigns, masquerade domains may be utilized in initial lures, although it is understood that spear phishing campaigns mimicking webmail or account security notifications are common. As is the norm in spear phishing campaigns of this nature, lures are sent to the victim that convey a sense of urgency, such as fake warnings of unauthorized access attempts to the victim's account that, if clicked, will lead to phishing sites that mimic the legitimate service and are used to harvest the victim's credentials.

Furthermore, watering hole attacks have been observed that involve the compromise of blogs and news sites that match the target demographic in an attempt to load malicious scripts that could exploit the visitors.

In addition to the email and watering hole vectors, it is also understood that the group have created fake social media profiles which are then used to engage with potential targets. As is common in such activities, the fake personas attempt to appeal to the target individual through simple flattery, 'attractive' profile images and claims of a shared interest.

Those victims that have their devices compromised have been observed as being targeted by 'DownPaper' (S0186), a backdoor trojan that uses the PowerShell to both execute (T1086) and maintain persistence (T1060). Subsequently, basic victim (T1033) and system information (T1082) is gathered and the malware features capabilities to download additional malicious payloads.

Recommendations

In addition to understanding and taking steps to mitigate any identified Charming Kitten ATT&CK techniques that are considered critical within an organization's environment, the following key elements should be considered:

- 'At risk' individuals, such as academics, activists and journalists, especially those critical of the Iranian regime, should exercise extreme caution when engaging with new contacts via social media and should be wary of any unsolicited or unexpected email containing suspicious attachments or links
- When visiting unsolicited links, especially when prompted for credentials, users should verify that they are on the legitimate website, or, manually enter correctly the expected URLs to ensure it is legit
- Standard users should not be permitted to execute native tools, such as PowerShell or others commonly used for system administration, to prevent their misuse in the event of an account being compromised

Cleaver (G0003)

Active since at least 2013, 'Cleaver' (Cylance[10]) has been attributed to Iran and, based on strong circumstantial evidence, is believed to be linked to 'Threat Group (TG-)2889' (SecureWorks[11]). In addition to targeting critical infrastructure worldwide, Cleaver has targeted the airline industry along with defense, healthcare, technology and telecommunications. Whilst significant amounts of data has been stolen from victims, likely of benefit to the Iranian state, it is also understood that attacks against critical infrastructure and industrial control systems (ICS) were intended to cause physical damage, potentially in retaliation for similar destructive attacks against Iran such as Stuxnet.

Based on Cleaver's observed activities, the following MITRE ATT&CK™ Techniques have been identified (Figure 5).

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Spearphishing Attachment	Command-Line Interface	New Service	New Service	Disabling Security Tools	Brute Force
Spearphishing Link	Service Execution	Registry Run Keys / Startup Folder			Credential Dumping
		Shortcut Modification			Input Capture

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
	Windows Admin Shares	Clipboard Data			
		Input Capture			
		Screen Capture			

Figure 5 – Cleaver (G0003) – Identified MITRE ATT&CK™ Techniques

Notable Campaign: Operation Cleaver

Cleaver, and the operation of the same name, somewhat expectedly utilizes some TTP elements that are consistent with other Iranian threat groups.

In order to target victims, it is understood that fake LinkedIn profiles, including fake personas with associated photos, personal details and social network connections, were created as a means to distribute malware, through social engineering techniques, to victims at the target organizations. Additionally, given that many

[10] https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

[11] https://www.secureworks.com/research/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles

organizations were subject to various systems being compromised, it is likely that social media intelligence (SOCMINT) gathering was also conducted using these profiles.

Of the personas identified during these campaigns, primary personas with comprehensively complete profiles are supported by secondary, less established, personas. Cleaver, utilizing these primary personas, would then engage with potential victims and their profiles would likely stand up to casual scrutiny, especially given that many social network users would not delve deeply into the profile's social network connections. Subsequently, as victims were lured into connecting with the primary persona, the rogue account effectively gains more legitimacy and would then withstand greater scrutiny and appeal to others that are familiar with existing victims.

Whilst many savvy individuals may be less inclined to connect with unknown personas on social networks such as LinkedIn, it is understood that many of the Cleaver personas masqueraded as 'recruiters' which would provide an adequate pretext for many to accept the connection.

As seen in other Iranian nexus campaigns, social engineering campaigns following an initial contact via social media have included fake job advertisements and the creation of masquerade domains mimicking legitimate organizations. Having lured a victim into applying for a fictious vacancy, custom payloads are deployed that reportedly include credential dumping (T1003) capabilities as well as features to enable lateral movement.

Furthermore the use of common tools such as 'Mimikatz' (S0002) and 'PsExec' (S0029) has been observed along with custom tools such 'Net Crawler' (S0056), an intranet worm used to brute force (T1110) credentials across the victim network, and 'TinyZbot' (S0004), a backdoor that captures both keyboard input (T1056) and screenshots (T1113) from the victim.

Recommendations

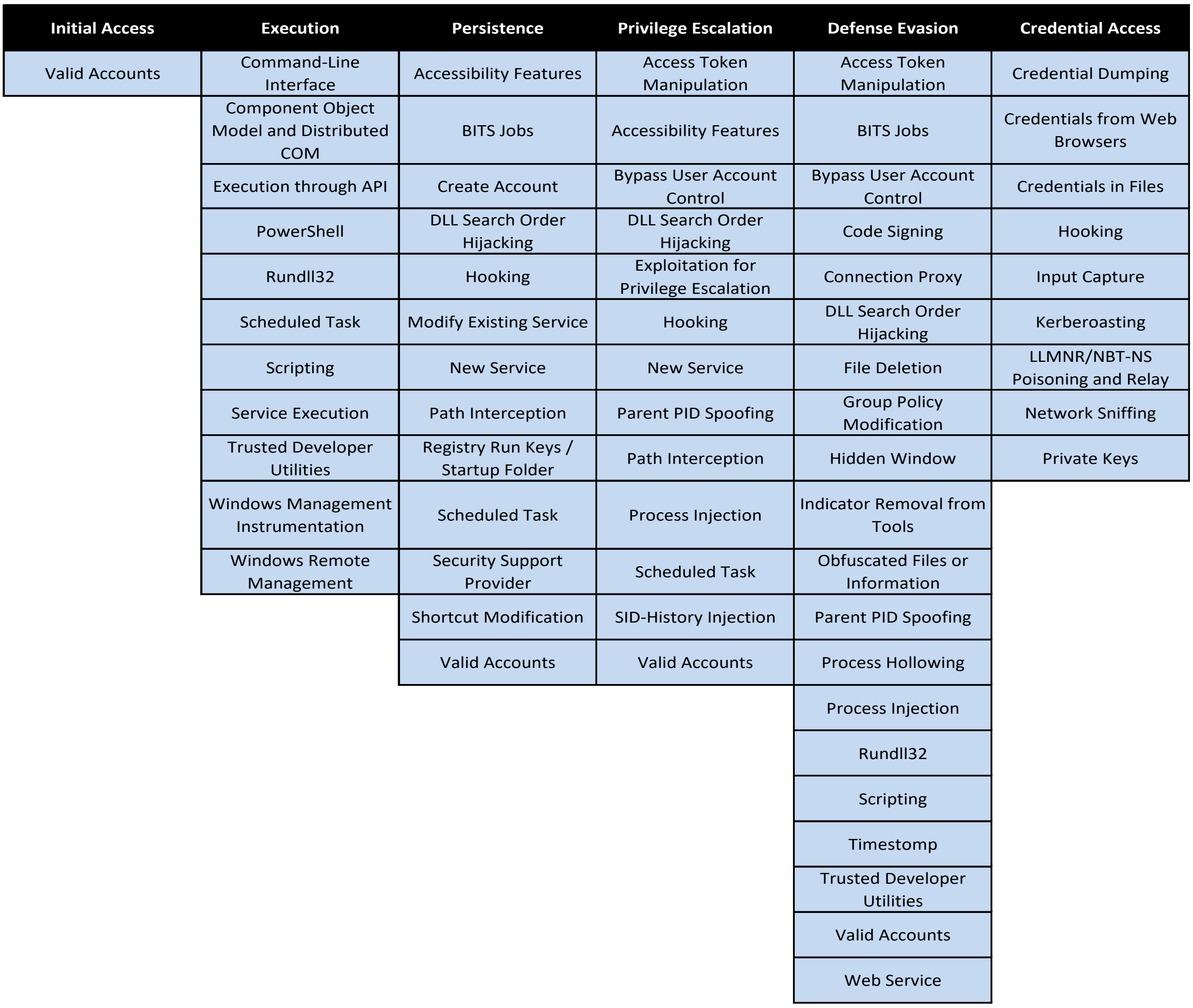
In addition to understanding and taking steps to mitigate any identified Cleaver ATT&CK techniques that are considered critical within an organization's environment, the following key elements should be considered:

- Whilst the use of social media outside of the workplace cannot be controlled, users should be advised to only interact with individuals that they know in the 'real world' and trust. In many cases this may not be entirely practical and as such, caution should be exercised when accepting files or links from untrusted sources – if in doubt, don't open or interact with suspicious third parties

CopyKittens (G0052)

Active since approximately 2013, 'CopyKittens' (ClearSky/Minerva Labs[12]) is an Iranian cyberespionage group that has targeted organizations in Israel, Germany, Jordan, Turkey, Saudi Arabia and the United States.

Based on CopyKittens' observed activities, the following MITRE ATT&CK™ Techniques have been identified (Figure 6).



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Valid Accounts	Command-Line Interface	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Credential Dumping
	Component Object Model and Distributed COM	BITS Jobs	Accessibility Features	BITS Jobs	Credentials from Web Browsers
	Execution through API	Create Account	Bypass User Account Control	Bypass User Account Control	Credentials in Files
	PowerShell	DLL Search Order Hijacking	DLL Search Order Hijacking	Code Signing	Hooking
	Rundll32	Hooking	Exploitation for Privilege Escalation	Connection Proxy	Input Capture
	Scheduled Task	Modify Existing Service	Hooking	DLL Search Order Hijacking	Kerberoasting
	Scripting	New Service	New Service	File Deletion	LLMNR/NBT-NS Poisoning and Relay
	Service Execution	Path Interception	Parent PID Spoofing	Group Policy Modification	Network Sniffing
	Trusted Developer Utilities	Registry Run Keys / Startup Folder	Path Interception	Hidden Window	Private Keys
	Windows Management Instrumentation	Scheduled Task	Process Injection	Indicator Removal from Tools	
	Windows Remote Management	Security Support Provider	Scheduled Task	Obfuscated Files or Information	
		Shortcut Modification	SID-History Injection	Parent PID Spoofing	
		Valid Accounts	Valid Accounts	Process Hollowing	
				Process Injection	
				Rundll32	
				Scripting	
				Timestomp	
				Trusted Developer Utilities	
				Valid Accounts	
				Web Service	

[12] https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Account Discovery	Comoonent Object Model and Distributed	Clipboard Data	Commonly Used Port	Data Compressed	
Browser Bookmark Discovery	Exploitation of Remote Services	Data from Local System	Connection Proxy	Data Encrypted	
Domain Trust Discovery	Pass the Hash	Email Collection	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	
File and Directory Discovery	Pass the Ticket	Input Capture	Multiband Communication	Exfiltration Over Command and Control Channel	
Network Service Scanning	Remote Desktop Protocol	Man in the Browser	Remote File Copy	Scheduled Transfer	
Network Share Discovery	Remote File Copy	Screen Capture	Standard Application Layer Protocol		
Network Sniffing	Remote Services	Video Capture	Standard Cryptographic Protocol		
Process Discovery	Windows Admin Shares		Web Service		
Remote System Discovery	Windows Remote Management				
Security Software Discovery					
System Information Discovery					
System Network Configuration Discovery					
System Network Connections Discovery					

Figure 6 – CopyKittens (G0052) – Identified MITRE ATT&CK™ Techniques

Notable Campaign: Operation Wilted Tulip

Reported activity in mid-2017, dubbed 'Operation Wilted Tulip', detailed cyberespionage activity against strategic targets as being conducted by CopyKittens. Seemingly using a broad range of tactics, techniques and procedures (TTP) to achieve their objectives, victims were either subjected to spear phishing attacks or were targeted via watering hole attacks.

In the case of spear phishing attacks, emails containing weaponized Microsoft Word documents were sent to victims and exploited an at-the-time zero-day remote code execution vulnerability 'CVE-2017-0199'[13] to deliver malicious payloads. Adding further legitimacy to these lure emails, the group were observed as using accounts compromised through other attacks to send malicious payloads to new unsuspected victims, such as the account breach of a government employee at the Ministry of Foreign Affairs in Northern Cyprus that was subsequently used to send the malicious payloads to similar organizations worldwide.

The use of watering hole attacks, aside from being an effective attack vector, involved the compromise of legitimate websites that were then used to deliver exploits to their visitors. As is common in the compromise

[13] https://nvd.nist.gov/vuln/detail/CVE-2017-0199

of websites, automated SQL injection tools such as 'Havij' (S0224) and 'sqlmap' (S0225) are understood to have been used against compromised watering hole hosts in addition to commercial vulnerability scanners.

Incidents of this nature often target websites following reconnaissance of the intended target, knowing that the target will visit, or simply because the website's demographic *is* the intended target. Notably, Operation Wilted Tulip saw the websites of popular newspapers being targeted, making ideal watering holes as many will visit daily, and injected malicious JavaScript links. Utilizing their own infrastructure, these injected links caused other malicious JavaScript code to be executed and performed intelligence gathering, social engineering and web exploitation of specific target visitors. To evade casual inspection, masquerade domains were used to host the malicious scripts, mimicking legitimate sites through name variations or homograph attacks.

Given the number of visitors to high-profile websites such as those compromised in this campaign, including national newspapers, government ministries and academia, it is understood that target whitelisting was used. Aside from ensuring that malicious content is only delivered to visitors from a target organization's IP address ranges, this method also reduces the risk of exposure when compromise *all* visitors.

Furthermore, and as seen in other Iranian-nexus cyberoperations, social media played a part in this operation with links to masquerade domains, mimicking legitimate newspapers, being distributed amongst social media groups as well as the creation of 'attractive' fake profiles and personas that were believed to be used to lure potential victims into interactions. Whilst the report detailing Operation Wilted Tulip did not detail specific malicious content being distributed via social media or the masquerade domains, it is surmised that target individuals may have received communications via private channels after a level of trust was established between them and the fake persona.

Payloads utilized in this campaign, much like other Iranian nation-state sponsored group activity, included the commercial off-the-shelf penetration testing tool 'Cobalt Strike' (S0154), an open-source post-exploit tool 'Empire' (S0363) and CopyKittens' own backdoor known 'TDTESS' (S0164).

As with most cyberespionage campaigns, the payloads delivered would have permitted lateral movement as well as the collection of data from any compromised host. Based on other Iranian espionage activity, it is likely that they sought data that could be used to gather intelligence on persons of interest or intelligence that could be leveraged by the Iranian state and military.

Recommendations

In addition to understanding and taking steps to mitigate any identified CopyKittens' ATT&CK techniques that are considered critical within an organization's environment, the following key elements should be considered:

- Whilst watering-hole attacks are a consequence of third-party compromise, web security mitigations should be considered, for example blocking access to sites with no or low reputations as well as preventing the execution of scripts from untrusted sources
- Security awareness training can help individuals better protect themselves from social engineering and social media threats such as exercising caution when interacting with unknown and untrusted individuals

Group5 (G0043)

First discovered in late 2015, 'Group5' (CitizenLab[14]) is a suspected Iranian nation-state sponsored threat actor that has targeted individuals within Syria that are opposed to the Syrian Government and President Assad regime. Unlike other cyber campaigns being conducted within Syria at the time, these threat group appeared to utilize different tactics, techniques and procedures along with Iranian indicators such as language within tools and the use of both Iran-based hosting providers and IP address ranges.

Based on Group5's observed activities, the following MITRE ATT&CK™ Techniques have been identified (Figure 7).

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
				File Deletion	Input Capture
				Obfuscated Files or Information	
				Software Packing	

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
		Input Capture	Uncommonly Used Port		
		Screen Capture			

Figure 7 – Group5 (G0043) – Identified MITRE ATT&CK™ Techniques

Whilst the attribution to Iran is circumstantial, it is believed that given the two nations share a strategic relationship, the cyber capabilities of Iran may have been utilized to target individuals opposed to President Bashar al-Assad.

As observed in other Iranian-nexus campaigns, initial attack vectors include the delivery of spear-phishing emails containing weaponized lure files as well as the creation of a watering hole website that copied content from other opposition websites to appear legitimate and hosted exploits and malware for both Windows and, presumably to target mobile users, Android.

Having been compromised, common remote access tools were deployed including 'njRAT' (S0385) and 'NanoCore' (S0336) which target Windows users as well as 'DroidJack' (S0320), an Android-based threat that has been observed as mimicking popular mobile applications in the past.

[14] https://citizenlab.ca/2016/08/group5-syria/

Recommendations

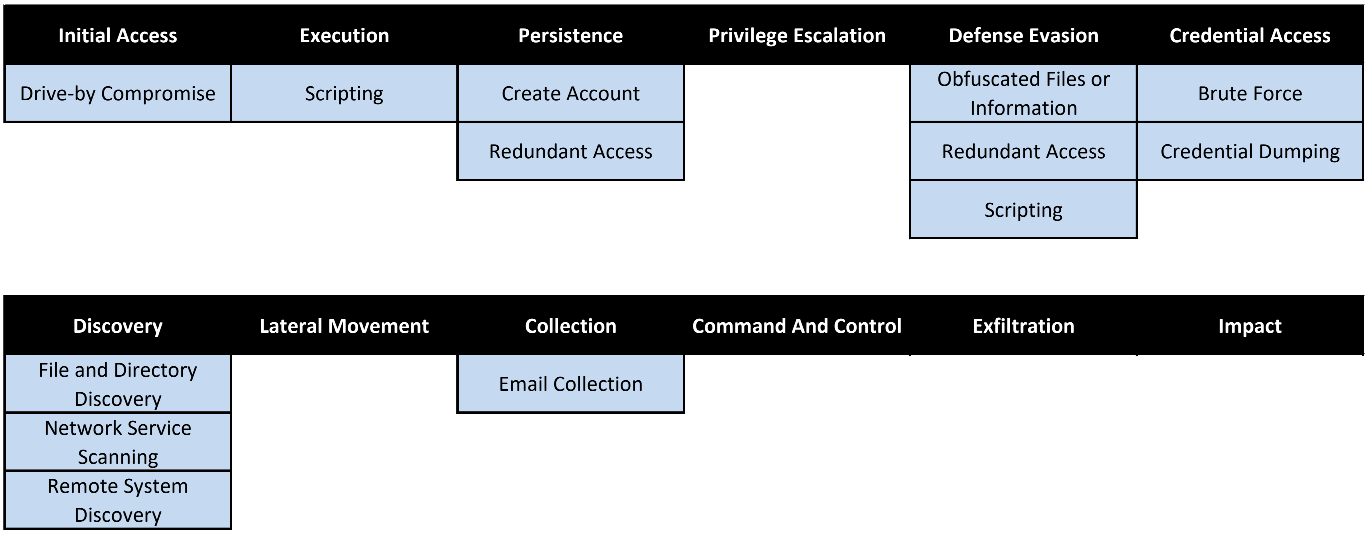
In addition to understanding and taking steps to mitigate any identified Group5 ATT&CK techniques that are considered critical within an organization’s environment, the following key elements should be considered:

- Whilst the politically-motivated targets of this campaign were individuals opposed to the Syrian regime, the use of mobile threats such as DroidJack may be utilized in other campaigns, as such, caution should also be exercised when installing mobile applications to ensure that they are both legitimate and their permissions do not exceed their requirements
- Additionally, the installation of applications downloaded from untrusted sources, such as third-party marketplaces, be that on personal or corporate devices should be discouraged

Leafminer (G0077)

Active since at early 2017, 'Leafminer' (Symantec[15]), also known as 'Raspite' (Dragos[16]) is an Iranian threat group that has targeted governments along with the financial and petrochemical industries across the Middle East.

Based on Leafminer's observed activities, the following MITRE ATT&CK™ Techniques have been identified (Figure 8).



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	Scripting	Create Account		Obfuscated Files or Information	Brute Force
		Redundant Access		Redundant Access	Credential Dumping
				Scripting	

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
File and Directory Discovery		Email Collection			
Network Service Scanning					
Remote System Discovery					

Figure 8 – Leafminer (G0077) – Identified MITRE ATT&CK™ Techniques

Similar to other Iranian cyberespionage campaigns, Leafminer has been observed as using both publicly available tools and custom malware threats although, the broad scale of their operation is believed to distinguish them from other suspected Iranian nation-state threat groups. Whilst initially detected within Symantec's telemetry on less than fifty systems, the discovery of the group's staging server, hosting tools, malware and vulnerability scan logs, led to the identification of over eight-hundred potential targets as well as exposing the poor operational security of Leafminer. This staging server was reported as being hosted on a compromised webserver and was accessible through a web shell, presumably left behind by the threat actor, permitting access to all content.

Whilst compromised websites were believed to be used for watering hole attacks against target individuals, Leafminer has also conducted a number of vulnerability scans against target networks, attempting to exploit their discoveries, as well as brute-forcing (T1110) system logins using dictionary attacks.

In addition to using exploits for common vulnerabilities, Leafminer was also reported as attempting to utilize proof-of-concept exploits gathered from public sources, such as those leaked by the Shadow Brokers in April

[15] https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east

[16] https://www.dragos.com/blog/20180802Raspite.html

2017, and was observed as using EternalBlue, the leaked US National Security Agency (NSA) exploit, as a method of lateral movement.

Although custom malware payloads were reported as being discovered, Leafminer has utilized the open-source penetration testing tool 'MailSniper' (S0413) to search through the Microsoft Exchange mailboxes of compromised organizations, as well as the credential stealing (T1003) tools 'Mimikatz' (S0002) and 'LaZagne' (S0349) to gather data from compromised hosts. Furthermore, the legitimate Microsoft utility 'PsExec' (S0029) has been used, potentially to perform discovery tasks on remote systems within the target network.

Recommendations

In addition to understanding and taking steps to mitigate any identified Leafminer ATT&CK techniques that are considered critical within an organization's environment, the following key elements should be considered:

- The exploitation of common vulnerabilities is only possible when systems are not patched; Organizations should ensure that security updates are applied regularly, be they for external-facing systems exposed to vulnerability scans or internal systems with vulnerabilities that could permit lateral movement and widespread compromise
- Additionally, organizations should monitor for changes on their own web assets to ensure that rogue code, be that web injections or shells, is not being used to compromised others or host malicious attack infrastructure

Magic Hound (G0059)

Active since at least 2014, 'Magic Hound' (Palo Alto[17]), also known as, and/or associated with, 'Rocket Kitten', 'Ajax Security Team', 'Cobalt Gypsy', 'Newscaster Team' and 'APT35', is an Iranian nation-state sponsored threat group that typically targets a broad range of organizations in the Middle East and United States, including governments as well as the defense, engineering, business services and telecommunications industries.

Based on Magic Hound's observed activities, the following MITRE ATT&CK™ Techniques have been identified (Figure 9).

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Spearphishing Attachment	Command-Line Interface	Account Manipulation		File Deletion	Account Manipulation
Spearphishing Link	PowerShell	Registry Run Keys / Startup Folder		Hidden Window	Credential Dumping
Spearphishing via Service	Scripting			Obfuscated Files or Information	Input Capture
	User Execution			Scripting	
				Web Service	

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
File and Directory Discovery	Remote File Copy	Email Collection	Commonly Used Port	Data Compressed	
Process Discovery		Input Capture	Remote File Copy		
System Information Discovery		Screen Capture	Standard Application Layer Protocol		
System Network Configuration Discovery			Uncommonly Used Port		
System Owner/User Discovery			Web Service		

Figure 9 – Magic Hound (G0059) – Identified MITRE ATT&CK™ Techniques

Notable Campaign: Saudi Arabian Espionage

A persistent campaign primarily targeting organizations in, or dealing with, Saudi Arabia was identified as being active since at least mid-2016 and utilized custom tools as well as an open-source Python-based cross-platform remote access tool named 'Pupy'[18] (S0192) that could target users of Android, Linux, MacOS and Windows.

[17] https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/

[18] hxxps://github.com/n1nj4sec/pupy

Commencing with weaponized Microsoft Excel spreadsheets, presumably delivered via targeted spear phishing campaigns and utilizing decoy themes such as job vacancies, as seen in other Iranian-nexus campaigns, as well holiday greetings and mimicking official government documents sent from the Ministries of Commerce or Health.

Furthermore, it would appear that there has been some overlap in attack infrastructure with domains being used in this campaign also featuring in 'Shamoon' (S0140), also known as 'Disttrack', destructive malware attacks against Saudi Arabian organizations.

Notably, for command and control (C2) communications, Magic Hound was observed as dropping an Internet Relay Chat (IRC) bot which would allow a remote operator, connected to the same IRC chat channel, to issue commands to the compromised host. It is reported that this bot is similar to other Iranian-nexus threats, yet again illustrating a shared body of knowledge and common tactics, techniques and procedures (TTP) across Iranian cyber operations.

Recommendations

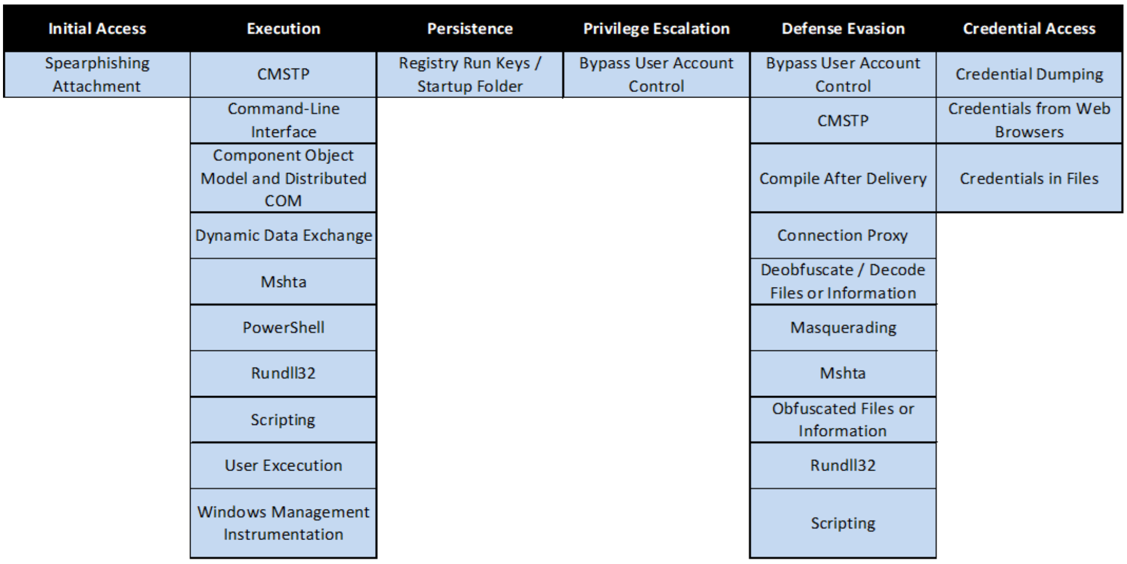
In addition to understanding and taking steps to mitigate any identified Magic Hound ATT&CK techniques that are considered critical within an organization's environment, the following key elements should be considered:

- Cross-platform threats such as used in operations conducted by Magic Hound demonstrate that it is not only Windows-users that are at risk, as such, suitable security controls should be considered for all deployed operating systems including mobile devices
- The legitimate use IRC may not be typical for many organizations and the application layer protocol and its associated ports should be considered for filtering

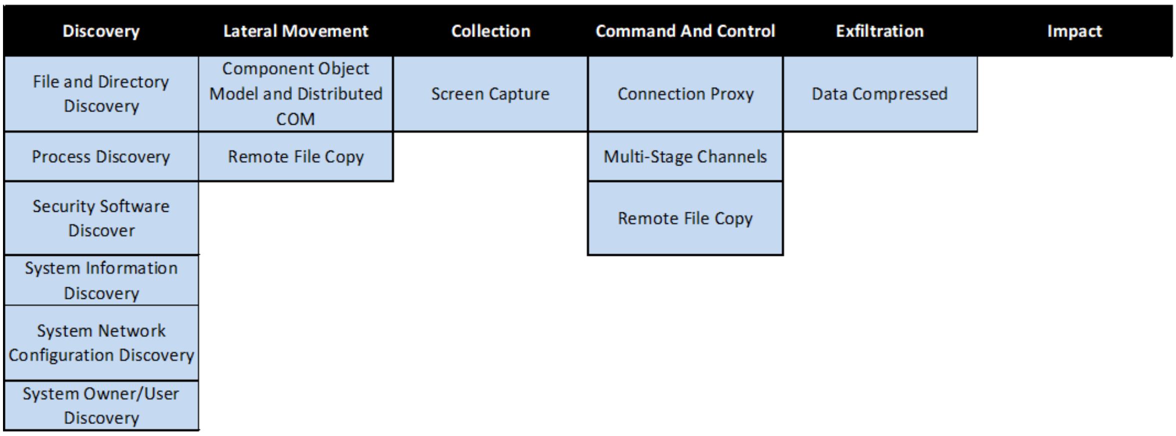
MuddyWater (G0069)

Active since at least 2017, 'MuddyWater' (Palo Alto[19]), also known as 'Seedworm' (Symantec[20]) and 'TEMP.Zagros' (Fireeye[21]), is an Iranian threat group that typically targets governments along with the telecommunications and oil industries primarily within organizations in the Middle East although Europe and North America have also been targeted.

Based on MuddyWater's observed activities, the following MITRE ATT&CK™ Techniques have been identified (Figure 10).



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Spearphishing Attachment	CMSTP	Registry Run Keys / Startup Folder	Bypass User Account Control	Bypass User Account Control	Credential Dumping
	Command-Line Interface			CMSTP	Credentials from Web Browsers
	Component Object Model and Distributed COM			Compile After Delivery	Credentials in Files
	Dynamic Data Exchange			Connection Proxy	
	Mshta			Deobfuscate / Decode Files or Information	
	PowerShell			Masquerading	
	Rundll32			Mshta	
	Scripting			Obfuscated Files or Information	
	User Excecution			Rundll32	
	Windows Management Instrumentation			Scripting	



Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
File and Directory Discovery	Component Object Model and Distributed COM	Screen Capture	Connection Proxy	Data Compressed	
Process Discovery	Remote File Copy		Multi-Stage Channels		
Security Software Discover			Remote File Copy		
System Information Discovery					
System Network Configuration Discovery					
System Owner/User Discovery					

Figure 10 – MuddyWater (G0069) – Identified MITRE ATT&CK™ Techniques

[19] https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

[20] https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group

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

Notable Campaign: Data Leaks, Telecoms and Government

During May 2019 a group referring to themselves as 'Green Leakers' on the messaging platform Telegram attempted to sell access to MuddyWater tools and/or infrastructure. Whilst the authenticity was questioned, screenshots shared with the media appeared to show compromised 'MuddyC2' command and control (C2) infrastructure.

Seemingly unabated, MuddyWater operations appeared to continue following this alleged leak with weaponized documents being used to target academia, government organizations and the telecommunications industry in the Middle East during June 2019.

Using weaponized documents that attempt to exploit the remote code execution vulnerability 'CVE-2017-0199'[22], a vulnerability also exploited by CopyKittens, the spear phishing email and document themes would be tailored to the victim organization and were also observed as using email spoofing, masquerading as being sent from legitimate organizations.

When the lure documents were opened, the user would be socially engineering into enabled macros that were identified as deploying a multistage Microsoft PowerShell-based backdoor dubbed 'PowerStats' (S0223). Utilizing layers of encoding and obfuscation (T1140) to thwart analysis, the backdoor would initially gather system information (T1082) to identify the victim to MuddyWater's C2 infrastructure and would subsequently allow additional payloads, such as to gather and exfiltrate data, to be deployed to the victim.

Recommendations

In addition to understanding and taking steps to mitigate any identified MuddyWater ATT&CK techniques that are considered critical within an organization's environment, the following key elements should be considered:

- PowerShell-based threats require the interpreter to be present and, as such, organizations not using it for legitimate administrative purposes could consider its removal
- Where PowerShell is required, code signing can be used to ensure that only trusted scripts are executed in addition to PowerShell 'remoting' security to limit remote executions[23]

[22] https://nvd.nist.gov/vuln/detail/CVE-2017-0199

[23] https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/winrmsecurity?view=powershell-7

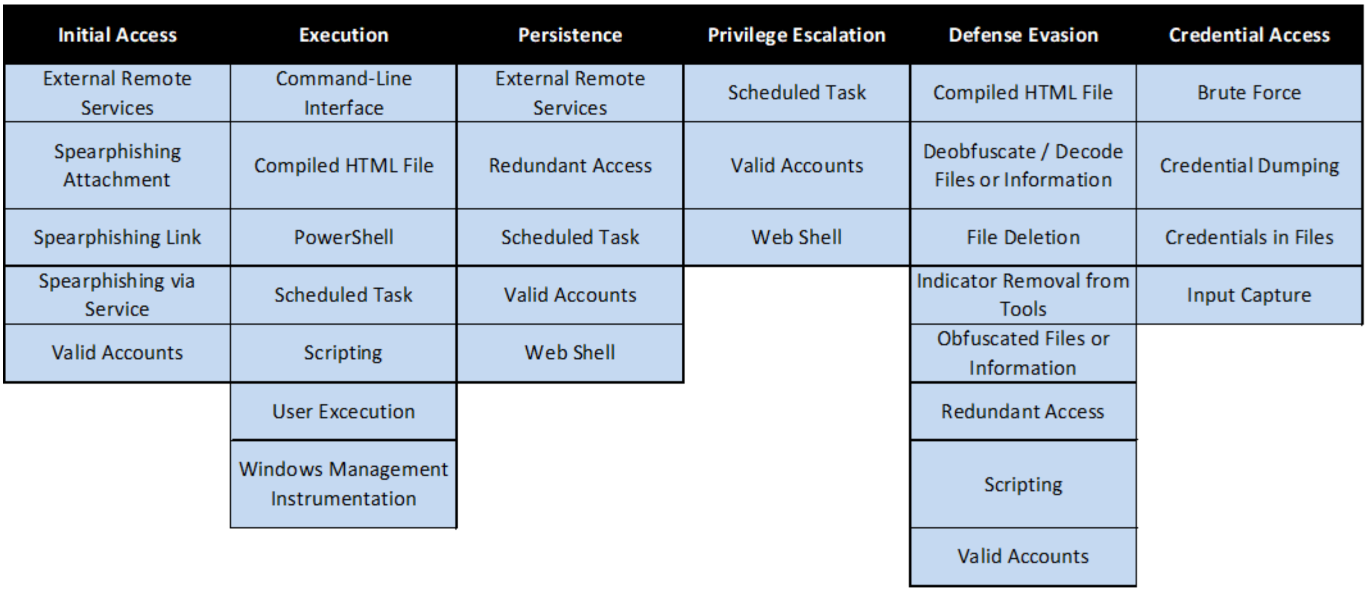
OilRig (G0049)

Active since at least 2014, 'OilRig' (Palo Alto[24]), also known as 'APT34' (Fireeye[25]) and 'Helix Kitten' (Crowdstrike[26]), is a suspected Iranian threat group that predominantly targets organizations in the Middle East including governments along with the telecommunications and oil industries. In addition to using infrastructure that references Iran, OilRig has been observed as using supply chain attacks against target organizations, a tactic which exploits the trusted relationship between a third party and the potential victim.

Much like legitimate software developers, OilRig reportedly undertakes a continuous development and evolution lifecycle for their toolset as well as the tactics, techniques and procedures (TTP) utilized in cyberespionage operations. Given this, past OilRig events likely serve as an indicator of past capability and future attacks may use enhanced TTP.

Initially the campaigns associated with 'APT34' and 'OilRig' were tracked separately but, following additional reporting, the groups were combined given increased confidence in their overlap.

Based on OilRig's observed activities, the following MITRE ATT&CK™ Techniques have been identified (Figure 11).

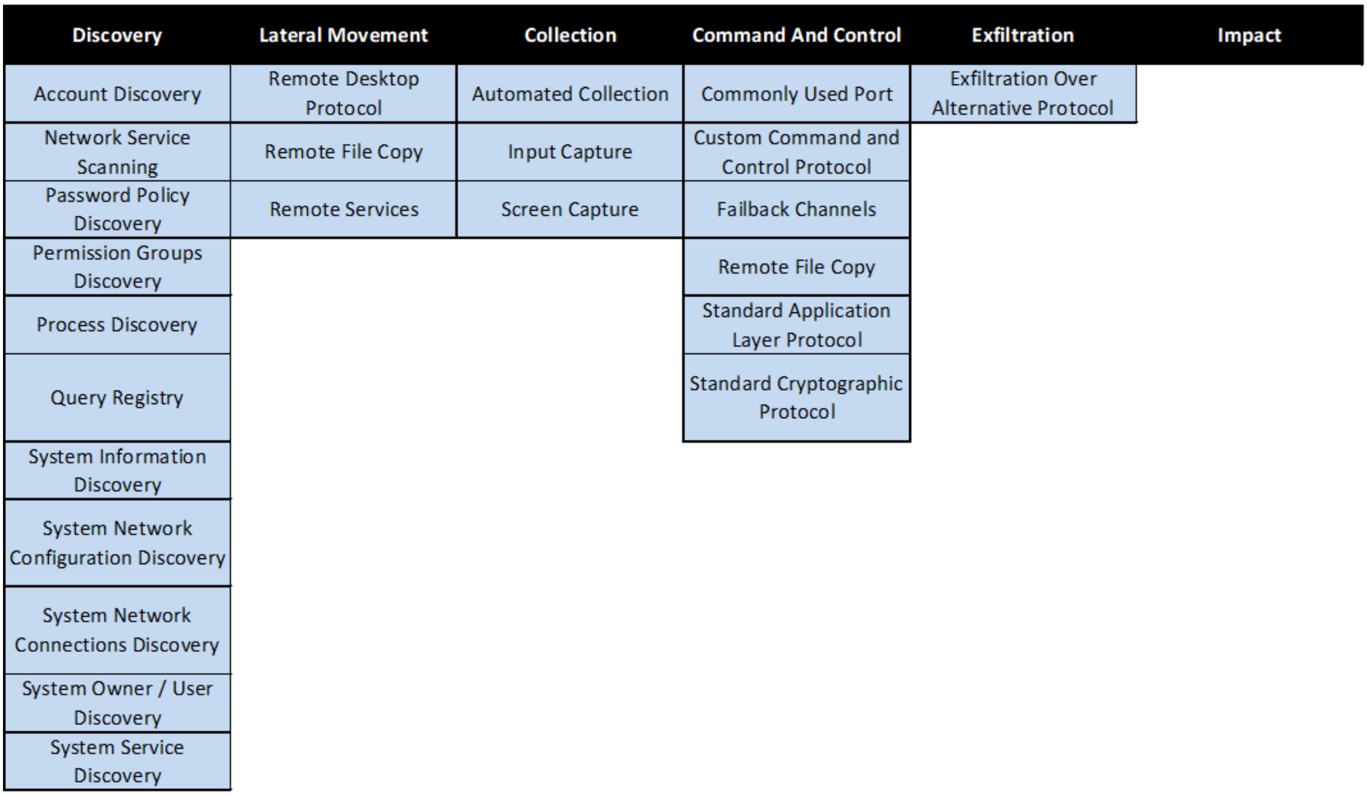


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
External Remote Services	Command-Line Interface	External Remote Services	Scheduled Task	Compiled HTML File	Brute Force
Spearphishing Attachment	Compiled HTML File	Redundant Access	Valid Accounts	Deobfuscate / Decode Files or Information	Credential Dumping
Spearphishing Link	PowerShell	Scheduled Task	Web Shell	File Deletion	Credentials in Files
Spearphishing via Service	Scheduled Task	Valid Accounts		Indicator Removal from Tools	Input Capture
Valid Accounts	Scripting	Web Shell		Obfuscated Files or Information	
	User Execution			Redundant Access	
	Windows Management Instrumentation			Scripting	
				Valid Accounts	

[24] https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

[25] https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

[26] https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/



Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Account Discovery	Remote Desktop Protocol	Automated Collection	Commonly Used Port	Exfiltration Over Alternative Protocol	
Network Service Scanning	Remote File Copy	Input Capture	Custom Command and Control Protocol		
Password Policy Discovery	Remote Services	Screen Capture	Failback Channels		
Permission Groups Discovery			Remote File Copy		
Process Discovery			Standard Application Layer Protocol		
Query Registry			Standard Cryptographic Protocol		
System Information Discovery					
System Network Configuration Discovery					
System Network Connections Discovery					
System Owner / User Discovery					
System Service Discovery					

Figure 11 – OilRig (G0049) – Identified MITRE ATT&CK™ Techniques

Notable Campaign: Evolving TTP and QUADAGENT

Observed during 2018, OilRig were observed as using a compromised Middle Eastern government agency from which to launch attacks against other organizations, specifically sending spear phishing emails to another government agency along with a technology services provider. Likely utilizing compromised accounts, be they from previous campaigns or credential harvesting/stuffing attacks, the use of a 'trusted' platform from which to launch attacks against others will undoubtedly improve the chance of initial access, especially if the target already has dealings with the compromised organization.

Whilst the use of a compromised third-party may be part of a specific supply chain attack, exploiting a third-party deemed to be 'weaker' in order to take advantage of any trust relationships, OilRig may also be using this tactic as a more opportunistic capability, assimilating a victim, completing any objectives, and then abusing their resources and status against the next victim.

As is common with most attacks, spear phishing emails appear to be the initial vector although, notably in this campaign, it is understood that the initial victim email addresses were not necessarily public knowledge. Whilst the email address format for many organizations can be brute-forced, through a combination of open source intelligence gathering and application to common formats such as '<firstname>.<lastname>@' or '<initial><lastname>@', it is suggested that in this instance OilRig may have collated potential victim recipients from other compromised mail accounts.

Similar to other Iranian-nexus threat groups, or potentially influencing or driving the attack technology used by their peers, OilRig was observed as using PowerShell and script-based backdoor payloads such as the custom developed 'QUADAGENT' tool (S0269). Based on third-party analysis of these backdoors, and CyberInt research analysis of other suspected Iranian PowerShell payloads, the use of the open-source 'Invoke-Obfuscation'[27] has been used to obfuscate their scripts and complicate analysis.

Once the QUADAGENT payload is executed, reportedly without displaying any decoy content, the creation of scheduled tasks (T1053) facilitates persistence and communications are established to the threat actor's command and control (C2) infrastructure using standard network protocols (T1043) including HTTPS, HTTP and subsequently DNS tunneling. The use of multiple protocols also provides fallback (T1008) capabilities to the backdoor, should one fail another can be used.

The absence of decoy content differs to many other Iranian-nexus campaigns and is presumably effective as decoys need to be kept 'fresh' in order to convince the recipient that nothing nefarious is occurring. In this instance, the lack of any visible activity may convince the victim that something hasn't worked, or they may not be aware that any action has occurred, leaving the threat to go about its malicious business.

Recommendations

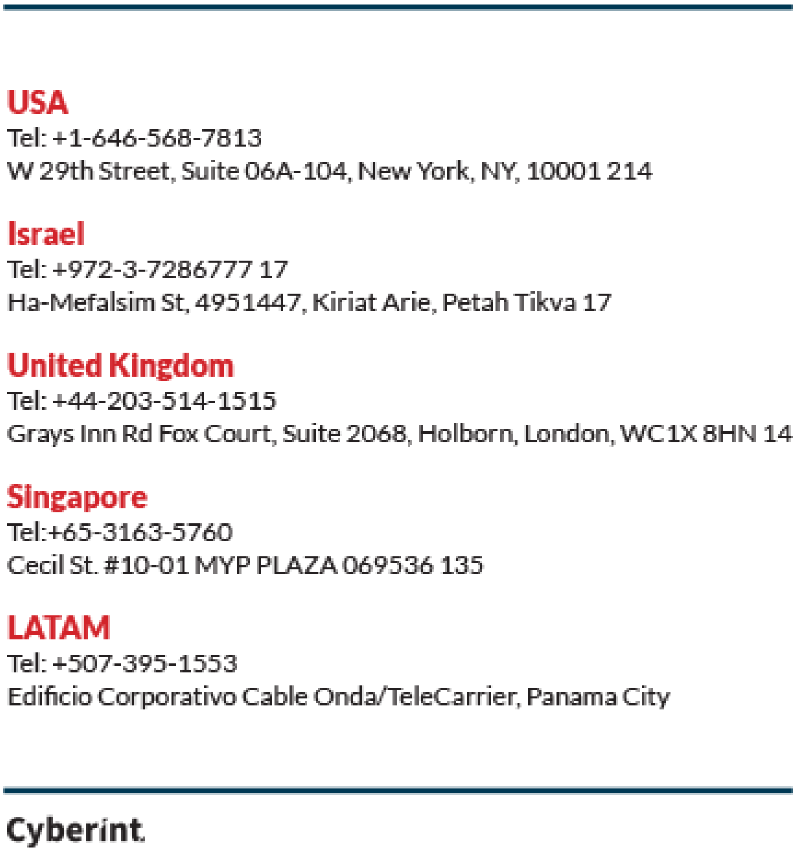
In addition to understanding and taking steps to mitigate any identified Charming Kitten ATT&CK techniques that are considered critical within an organization's environment, the following key elements should be considered:

- As with other PowerShell-based threats, organizations should take steps to remove or restrict access to PowerShell on endpoints
- With the suggestion that mailboxes of third-party organizations were compromised to launch attacks against others, simple measures such as educating users on the dangers of password reuse can thwart the credential harvesting and stuffing attacks used to achieve this
- Furthermore, controls such using multi-factor authentication on public-facing email services or only allowing access to corporate assets through the use of virtual private networks (VPN) may further prevent the misuse of infrastructure in attacks against other organizations

[27] https://github.com/danielbohannon/Invoke-Obfuscation

Contact Information

www.cyberint.com | sales@cyberint.com | blog.cyberint.com



USA
Tel: +1-646-568-7813
W 29th Street, Suite 06A-104, New York, NY, 10001 214

Israel
Tel: +972-3-7286777 17
Ha-Mefalsim St, 4951447, Kiriat Arie, Petah Tikva 17

United Kingdom
Tel: +44-203-514-1515
Grays Inn Rd Fox Court, Suite 2068, Holborn, London, WC1X 8HN 14

Singapore
Tel:+65-3163-5760
Cecil St. #10-01 MYP PLAZA 069536 135

LATAM
Tel: +507-395-1553
Edificio Corporativo Cable Onda/TeleCarrier, Panama City

Cyberint