THREAT INTELLIGENCE REPORT

The Iran Threat, In Brief

By Adam Hlavek

Since the Iranian Revolution and the establishment of the current Islamic Republic in 1979, Iranian leadership has been in near constant conflict with the West and several of its Middle Eastern neighbors. The United States' previous alliance with the overthrown Pahlavi dynasty and the ensuing hostage crisis set the stage for the tensions that would follow between the two nations in the coming decades. The U.S. and its allies' efforts to contain, counter, and undermine the regime's influence have taken a variety of forms, including diplomacy, legal action, and economic sanctions. Iran's determination to establish itself as a nuclear power has also exacerbated the West's growing concern over the rogue nation's military ambitions.

Thus, the 2010 discovery of a sophisticated and largely unprecedented cyber sabotage campaign targeting Iran's nuclear facilities at Natanz would prove pivotal in the relationship between the U.S. and the Islamic Republic. While the U.S. government has never claimed responsibility for the Stuxnet virus that disabled hundreds of Iranian centrifuges, many have asserted that the operation was the work of U.S. and/or Israeli intelligence. This debate aside, Iranian officials wasted little time in publicly blaming the U.S. and Israel for the attacks.

Following the Stuxnet attacks, Iran set itself on a course to aggressively develop its own cyberspace capabilities. Lacking the military and economic might of its Western rivals, Iranian leadership views cyber as an asymmetrical tool to do damage to their enemies and effectively gather intelligence on foreign governments, corporations, academic institutions, and non-governmental organizations (NGO) abroad, in addition to their own citizens. Once viewed as cyberspace "amateurs," the Iranian intelligence apparatus has steadily and conspicuously grown its domestic cyber know-how. While Iranian cyber operators may not be viewed as top tier in terms of their technical sophistication, the regime's willingness to conduct aggressive and destructive cyber operations dramatically increases the potential threat posed to those in the crosshairs. Highly disruptive operations presumably carried out at the behest of the Ayatollah have included drive-wiping attacks against Saudi oil companies and large-scale denial of service attacks against the U.S. financial sector. These actions have displayed open contempt for international norms and indicate the regime's willingness to retaliate for a variety of perceived transgressions within the cyber domain.

As the last two years have given witness to dozens of malicious cyber campaigns attributed to numerous Iranian actors, it appears the regime's plan has come full circle: cyber has become a full-fledged, core component of Iran's strategy to harass, contest, and punish its adversaries around the Middle East and the globe.

Iran’s Strategic Goals

1. Escape International Sanctions and Modernize the Economy

Iran’s economy has struggled following the years of sanctions imposed by the United Nations, the U.S., and U.S. allies. The latest round of sanctions imposed due to the dissolution of the Joint Comprehensive Plan of Action (JCPOA) nuclear deal have been particularly hard-hitting, sending the Iranian economy into a deep recession.

To that end, Iran is seeking economic alliances outside the Western sphere of influence. Most notably, Iran is apparently entering into a $400 billion investment agreement with China that would include infrastructure investment and cooperation on defense and intelligence initiatives.

Iran has also been willing to pursue intellectual property theft via cyber operations as a means of enhancing its competitive advantage, demonstrating a particular focus on defense and information technologies. A 2018 report from the U.S. National Counterintelligence and Security Center highlights this threat, stating “Iran will continue working to penetrate U.S. networks for economic or industrial espionage purposes. Iran’s economy—still driven heavily by petroleum revenue—will depend on growth in non-oil industries and we expect Iran will continue to exploit cyberspace to gain advantages in these industries.”

Historical Cyber Examples:

- 2018: Mabna Institute Indictment

Recent Cyber Examples:

- OilRig
- APT33
- 2020: IP Theft Indictments
- 2020: Targeting of COVID-19 Research

2. Defeat Regional Adversaries in the Middle East

While Iran’s diplomatic relationships with its regional neighbors have differed over time and from state-to-state, Iranian leadership has consistently sought to undermine and contest nations within the region that it sees as direct rivals. Seeking to establish itself as the preeminent power in the region, Tehran has repeatedly chafed against Israel and Sunni-led states allied with the U.S. such as Saudi Arabia, Bahrain, and the United Arab Emirates. These conflicts have taken several forms, from economic and diplomatic disputes to outright military confrontation. The Islamic Republic has also actively supported insurgent militant groups such as Hezbollah in Lebanon and the Houthi rebels in Yemen as a means to asymmetrically fight battles against their adversaries via proxy forces, as the regime cannot afford the political and military costs of conventional warfare.

Cyberspace has also provided a new and appealing domain for the Iranian military and intelligence services to leverage, as it offers a low barrier to entry and often makes identifying those responsible difficult. Thus, many of the recent cyber intrusion campaigns linked to Iran have targeted governments, corporations, and NGOs within the Middle East. These campaigns serve multiple purposes: to collect information on organizations and individuals of interest to the Iranian intelligence services, to gain economic and political advantage, and, in the most extreme cases, to damage or destroy information systems or operational technology.

Historical Cyber Examples:

- 2012: Shamoon Attacks on Saudi Aramco and RasGas
- 2016: Shamoon 2 Attacks Against Saudi Arabia

Recent Cyber Examples:

- OilRig
- MuddyWater

3. Preserve the Ayatollah's Regime and Quell Dissent

Post-revolutionary Iran has a well-documented history of highly centralized control of information and censorship. With dedicated government ministries overseeing the various forms of media, the regime's leadership requires strict adherence to the tenets of Shia Islam and forbids any significant criticisms of the Supreme Leader and his government. Reporters Without Borders has consistently ranked Iran as one of the most repressive countries in the world with regard to press freedoms.

Economic and political disenfranchisement have sparked multiple public protest movements in Iran over the past decade, from protests in 2009 stemming from Iranian President Mahmoud Ahmadinejad's election victory to 2019 protests initially spurred by dramatic increases in gasoline prices. Regime leadership has frequently responded to these demonstrations with brutal military force.

Iranian authorities have also proven to be more than willing to use technology to censor and surveil their citizenry. Some notable examples include the government essentially cutting off Internet access across the country in November 2019 in response to widespread protests and likely being responsible for the compromise of certificate authority DigiNotar in 2011, which resulted in thousands of Iranian Google users being redirected to look-a-like webpages. Such actions underscore the regime's determination to maintain strict control over the flow of information within Iran's borders.

Historical Cyber Examples:

- 2009 - Twitter Defacement
- 2011 - DigiNotar Breach

Recent Cyber Examples:

- 2019 - Internet Shutdown
- 2020 - Indicted Regime-sponsored Hackers

4. Punish and Discredit Ideological Adversaries

The regime has also shown an affinity for highly destructive "revenge" attacks against its enemies, particularly Saudi Arabia and the United States. The Shamoon malware deployed against Saudi and Qatari oil and gas companies represents a watershed moment, as these attacks resulted in the effective sabotage of thousands of computer systems within the victims' corporate networks. Iranian operators are also believed to have been behind campaigns designed to disrupt a variety of U.S. government and private sector entities, to include banks, hotels, and most recently the U.S. presidential elections. Such cyber operations are likely designed to project power and serve as a warning to other nations or companies that are weighing their strategies for dealing with Iran.

While cyber-enabled espionage has become commonplace amongst world powers, Iran's actions to harm commercial and industrial entities abroad illustrate a disregard for international norms and a willingness to cross "red lines" not seen by other prominent cyber powers today.

Historical Cyber Examples:

- 2012 - Operation Ababil
- 2014 - Sands Casino attack

Recent Cyber Examples:

- OilRig
- 2020 - Global Disinformation Campaign

Recent Iranian Threat Campaigns

Fox Kitten

Overview

Between late 2019 and summer 2020, multiple sources have described intrusion activity attributed to Iranian state-sponsored cyber operators leveraging recently publicized vulnerabilities in popular virtual private network (VPN) services such as Pulse Secure, Fortinet, and Palo Alto's GlobalProtect. Researchers at ClearSky described these operations in early 2020, indicating this campaign has likely been active since 2017 and asserting overlaps between this group and other Iranian threat groups (APT33, Oilrig, and Chafer). The campaign included a wide range of targeted countries and industries, to include the information technology, telecommunications, oil and gas, aviation, government, and security sectors. The group appears focused on establishing the initial footholds within the victim networks and frequently relies on SSH tunneling to maintain persistence within those networks.

Recent Activity

In September 2020, CISA and the FBI appear to have corroborated these findings, releasing a technical alert attributing the successful exploitation of VPN infrastructure to the group and mapping the group's tactics, techniques, and procedures (TTP) to the MITRE ATT&CK Framework. While not explicitly naming the ties to Fox Kitten, CISA had released an earlier alert warning of the ongoing exploitation of vulnerabilities within F5 BIG-IP infrastructure, another TTP that has been used by the group.

Known Targets	Middle East and United States; Information Technology, Telecommunications, Healthcare, Financial, Media, Oil and Gas, Aviation, Government, and Security sectors
Sample TTPs	Exploitation of VPNs and other network appliances
	Use of SSH tunneling to facilitate RDP access to victims
	The use of custom, open source, and legitimate native software tools
Also Known As	Pioneer Kitten and PARISITE

OilRig

Overview

The OilRig group has been a prolific threat actor within the Middle East for several years. OilRig has primarily targeted Middle Eastern organizations, but has also on occasion targeted those outside the region, including the United States. The group is assessed to be operating on behalf of the Iranian government based on technical indicators and targeting patterns that closely align with Iranian interests.

The group's tactics have continued to evolve over time. OilRig has used a combination of proprietary malware, customized versions of publicly available hacktools, and "off the shelf" software. Social engineering has featured prominently in many of their campaigns, with the group leveraging social media platforms and masquerading as Western universities on multiple occasions.

OilRig has also been potentially linked to the infamous Shamoon attacks that struck Saudi Arabian and Qatari targets in 2012 and 2016. While these links are not definitive, researchers at Symantec did find malware used by the group (tracked by Symantec as Greenbug) resident on the same system as the Shamoon 2 disk-wiping malware in 2016.

Recent Activity

Spring 2020 witnessed OilRig incorporate new tactics into their operations, with researchers noting the use of both the DNS-over-HTTPS protocol and email attachments containing steganography for covert communication channels. Telecommunications companies have been among the group's recent targets, which falls in line with the group's historical focus on espionage enablement. The group's malware toolset has continued to evolve; a modified version of the TONEDEAF backdoor was used in early 2020 during a campaign imitating a U.S. professional services company known to contract with the U.S. government. 2020 also saw OilRig linked to another destructive wiper malware dubbed ZeroCleare, which was used in an attack against organizations within the energy and industrial sectors in the Middle East.

Known Targets	Middle East and United States; Energy, Public Utilities, Airlines, Financial, Chemical, Telecommunications, Government, and Oil and Gas sectors
Sample TTPs	Social engineering
	Spearphishing
	DNS exfiltration, using both custom-built and open-source software tools
	Extensive use of DNS tunneling for command and control (C2)
	Email-based C2 using Exchange Web Services and steganography to insert data and commands into image files attached to emails
	Credential harvesting and use of compromised accounts
Also Known As	APT34, Greenbug, Helix Kitten, and ITG13

APT33

Overview

APT33 has been highly active since 2015, targeting Iranian adversaries like commercial and governmental entities in Saudi Arabia and the United States, among others. The group has been observed using both advanced custom malware and publicly available hacktools to target sectors such as aviation and petrochemical production. APT33 has strong links to Iranian government entities based on the group's selection of targets and technical indicators linking an online persona to an Iranian cyber institute.

Notably, APT33 has been linked to destructive wiper malware more than once. The group deployed a wiper known as Stonedrill or SHAPESHIFT in 2016, which, like the earlier infamous Shamoon attacks, was used to target organizations in Saudi Arabia. In 2018, researchers at McAfee also asserted that they believed APT33 (or a group masquerading as them) were likely responsible for the 2012, 2016, and 2018 Shamoon attacks. While the precise attribution of these destructive tools is murky, Iranian state sponsorship appears to be the common thread.

Recent Activity

In late 2019, researchers at TrendMicro detailed activity attributed to APT33 in which the group established very narrowly targeted botnets to exploit their intended victims. This campaign appeared to follow previous APT33 patterns, as victims included U.S. private companies and universities, U.K. and European oil companies, and several victims in the Middle East and Asia. The campaign included phishing emails designed to impersonate known aviation, oil, and gas companies, which likely served as an initial infection vector. The APT33 actors also went to great lengths to obfuscate their infrastructure, using a series of bot controllers, VPNs, and cloud-hosted proxies to hide their activities.

Known Targets	United States, Saudi Arabia, and South Korea; Aviation, Manufacturing and Engineering, Energy, and Petrochemical
Sample TTPs	Spearphishing is a frequent initial intrusion vector
	Destructive (drive-wiping) malware
	Leveraging botnets, private VPNs, and cloud-hosted proxies to enhance obfuscation and operational security
Also Known As	Elfin, Magnallium, Holmium, and Refined Kitten

Chafer

Overview

Chafer is an Iran-linked threat group that has predominantly focused on the theft of data and personal information from targets in the Middle East and United States. The group has been active since at least 2015 and was particularly busy in 2017, targeting multiple sectors and nations across the Middle East, including a major telecommunications provider. The intrusion into the telecom provider suggests that Chafer's focus may be tracking and surveillance of end users or the establishment of initial accesses for follow-on operations.

In early attacks, Chafer operators were observed obtaining initial access via SQL injection attacks against internet-facing web servers. However, more recent campaigns document the use of spearphishing emails with malicious attachments such as Excel files. Historically, the group's command and control domains have masqueraded as legitimate Windows update service domains.

Multiple researchers have noted potential overlaps with OilRig, both in terms of shared command and control IPs and code overlaps. As is the case with many of the groups detailed here, such overlap amongst campaigns is likely inevitable, as the individuals behind them may share information, infrastructure, or intelligence requirements over time.

Recent Activity

In spring of 2020, researchers at Bitdefender identified campaigns perpetrated by Chafer that targeted air transportation and government entities in Saudi Arabia and Kuwait during 2018 and 2019. These campaigns appear to fall very much in line with previously reported Chafer activity, both in terms of the countries and sectors targeted and the continued interest in gathering intelligence and surveillance data on historic Iranian adversaries.

In September 2020, the U.S. Department of the Treasury announced sanctions against 45 Iranian nationals and a front company named Rana Intelligence Computing Company based on links to the Iranian Ministry of Intelligence and Security (MOIS). The Treasury Department specifically tied these sanctions to malicious campaigns conducted by Chafer targeting "Iranian dissidents, journalists, and international companies in the travel sector." The U.S. FBI also released a technical alert detailing a variety of malware known to be used by the group.

Known Targets	Telecommunications, Aviation, Government, Software, IT Services, and Travel sectors across multiple regions with a focus on the Middle East
Sample TTPs	Spearphishing using malicious hyperlinks or attachments
	SQL injection attacks via front-end web servers
	The use of custom backdoors (Remexi) combined with publicly available software tools
Also Known As	APT39

MuddyWater

Overview

MuddyWater is an Iran-linked threat group that has primarily targeted governmental entities, telecommunications companies, and information technology firms for espionage purposes since at least 2017. The group's targets have historically been centered in the Middle East, with Saudia Arabia specifically attributing a hacking campaign to the group. The group was also potentially tied to campaigns targeting Central Asia in 2018 and Eastern Europe in 2019.

The group primarily relies on publicly available tools for lateral movement, credential theft, and exfiltration and achieves initial access via spearphishing emails containing Word document attachments with macros to enable malicious payload delivery. MuddyWater has also continued to utilize and update a group of custom tools, many of which are scripts written in Python or PowerShell.

Recent Activity

In early 2020, researchers identified a MuddyWater-linked campaign dubbed "Summer Mirage." Based on the content and themes of the observed phishing emails and the attached malicious documents, the campaign may have targeted U.S. entities and the oil and gas sector. The malware used in this campaign also contained some new features, suggesting the group continues to update their preferred POWERSTATS PowerShell Trojan.

In October 2020, researchers at ClearSky identified a campaign targeting multiple Israeli organizations. The group attempted to install a malicious downloader known as PowGoop during this campaign. PowGoop was likely used during another recent intrusion into a Middle Eastern state-run organization in which an unidentified group of threat actors also deployed the Thanos ransomware. This activity suggests the presence of PowGoop may serve as a precursor to ransomware deployment. Not exclusively used by MuddyWater, the Thanos ransomware is known to have been bought and sold on dark web forums. Separate reporting has also highlighted ongoing MuddyWater campaigns targeting Middle Eastern entities and potential links to the PowGoop malware.

Since MuddyWater has not historically been observed conducting ransomware attacks, researchers speculate that the actual goal of the operation may have been to serve as a de facto destructive attack, akin to the NotPetya attacks of 2017 and similar to those carried out by other Iranian threat actors in the past. The use of ransomware could thus serve to hide the true motivations or culprits behind the attack.

Known Targets	Telecommunications, IT, Oil and Gas, NGOs, and the Middle East
Sample TTPs	Spearphishing
	Use and updating of PowerShell backdoor known as POWERSTATS
	Use of GitHub to store software tools
	Weaponization of stolen legitimate documents
Also Known As	Seedworm and TEMP.Zagros

Charming Kitten

Overview

Charming Kitten is an Iranian cyber espionage group largely known for their targeting of academics, human rights advocates, and members of the international media with a nexus to Iran. Believed to have been active since 2014, the group frequently uses social engineering techniques coupled with evolving technical TTPs to ensnare their victims. The group appears more focused on gaining information on the individuals they target than capturing troves of data like other Iranian cyber actors. In 2019, the group unsuccessfully targeted email accounts belonging to individuals associated with a U.S. presidential campaign and current and former U.S. government officials.

Recent Activity

While Charming Kitten has continued to target the same demographic groups, its operators have continued to adapt their tactics and attempted to use new communications platforms to interact with their targets. In summer of 2020, the group was observed using WhatsApp, LinkedIn, and even calling targets directly on the phone.

Charming Kitten actors have continued to attempt to infiltrate U.S. politics, most recently by accessing the accounts of individuals within the Trump administration and presidential campaign staff between May and June of 2020. The group was also linked to attempts to target the U.S. pharmaceutical company Gilead, which has garnered international media attention for the company's work researching treatments for COVID-19.

Known Targets	Academics, NGOs, human rights activists, and journalists predominantly within the Middle East, Europe, and the U.S.
Sample TTPs	Spearphishing
	Leveraging fake personas and social media platforms to interact with their targets
	Frequent impersonation of journalists
	Watering hole attacks using compromised legitimate websites that are relevant to their targeted victims
	Impersonations of popular online sites (Google, Microsoft, Yahoo) to harvest user credentials
	Phishing via SMS, WhatsApp, or social media sites
Also Known As	APT35, Ajax, and Phosphorus

In Summary

As outlined above, the past decade has seen the Iranian government rapidly adopt cyberspace operations as a primary tool of national power, demonstrate a strong willingness to use cyber as a weapon for retaliation, and rely upon cyber as a means for intelligence collection and espionage. The number of campaigns documented by the cybersecurity community in just the past two years illustrates the significant volume of operations being carried out at the direction of the regime's political and military leadership, which is particularly notable given the possibility that there are additional, ongoing intrusions that have yet gone undetected or undocumented in the public sphere.

As is almost always the case when discussing state-sponsored threats, the enterprises being victimized by Iranian hackers often lack the tools and information to systematically and effectively counter these adversaries. The growth in volume and sophistication exhibited by Iranian cyber operators suggests that the threat from these groups is continuing to accelerate. Countering such a threat calls for new and innovative forms of defense.

IronNet's mission is to drive such innovation and build the tools to defend companies, sectors, and nations against these kinds of global threats. Harnessing state-of-the-art behavioral analytics powering IronDefense, IronNet's Network Detection and Response (NDR) solution, and collaboratively sharing threat intelligence in real-time across enterprises via IronDome, IronNet's Collective Defense platform, provides IronNet's customers with unique capabilities to better detect and defend against such threats, whether originating from hostile nations or criminal networks.