

January 2020



THE IRAN CYBER PANIC

**How Apathy Got Us Here,
and What to Do Now**

Authored By:

Parham Eftekhari, Executive Director, ICIT

ICIT | Institute for Critical
Infrastructure Technology
The Cybersecurity Think Tank

The Iran Cyber Panic

How Apathy Got Us Here, and What to Do Now

January 2020

This paper would not have been possible without contributions from:

- Drew Spaniel, Lead Researcher, ICIT

ICIT would like to thank the following experts for their insights during the development of this paper:

- John Agnello, ICIT Contributor & Chief, Analytic Capability Development Branch, United States Cyber Command
- Jerry Davis, ICIT Fellow & Former CIO, NASA Ames Research Center
- Malcolm Harkins, ICIT Fellow & Chief Security and Trust Officer, Cymatic
- Itzik Kotler, Co-Founder & CTO at SafeBreach
- Ernie Magnotti, ICIT Fellow & CISO Leonardo DRS
- Luther Martin, ICIT Contributor & Distinguished Technologist, Micro Focus

Copyright 2020 Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the www.icitech.org website, and (3) certain other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

Table of Contents

Introduction	3
How A Lack of Prioritization Led to National Panic.....	4
Iran is Capable of a Significant Cyber Conflict – But How Far Will They Go?	4
Iran’s Understanding of US Military Capabilities Point to Cyber Retaliation.....	5
International Law May Influence Iranian Response	5
Iran’s Modus Operandi: Disruptive Attacks	6
Notable Iranian APTs.....	8
Operation Cleaver: Disassembled But Not Gone	8
APT33	9
Targeted Sectors	11
Disruption to Energy, Water, and Critical Manufacturing	11
The Defense Industrial Base	11
Financial Sector	12
Academia	12
The Healthcare Sector.....	13
Increased Attacks from Other Enemies & and The Importance of Attribution	14
Nation States and Cybercriminals Posing as Iran.....	14
Iran Posing as Other Bad Actors	14
Information Warfare	15
Mitigating Risk from Iranian Cyber Aggression.....	16
Monitor for the Common Stages of Iranian APT Campaigns	16
Immediate Cybersecurity Awareness Training for All Personnel	16
Disaster Recovery Wargames	17
Redundancy & Continuity of Operations	17
Assess the Security Posture & Prioritize Remediation.....	17
Practice Long-Term Vigilance.....	17
Basic Cyber Hygiene.....	18
Conclusion.....	18
Sources.....	19

Introduction

Since the January 2, 2020 drone strikes that killed Iranian General Qasem Soleimani, cyber and national security experts have worried about retaliatory cyberattacks against US interests. Today, organizations are preparing for the worst, as the potential for a major cyber incident looms large in the minds of government and private sector leaders alike.

An analysis of the Iranian government's strategic use of cyber-weapons over the past decade shows a history of exploiting digital vulnerabilities to cause disruption and conduct espionage. The logical conclusion is that more disruptive attacks are coming, but the severity of these attacks and the intended targets are uncertain. Adding further complexity to this discussion is Iran's network of proxies whose actions tend to be aligned with directions from Iran but who risk going rogue.

During this time of heightened risk and sensitivity to cyberattacks, the importance of attribution must also be revisited. The possibility exists that America's most resourceful and sophisticated adversaries, Russia and China, will take advantage of this crisis through false flag attacks or information warfare to further divide Americans and fan the flames of Iranian contempt. An example of this possibility occurred late last year, when the Russian advanced persistent threat (APT) Turla stole tools and infiltrated Iranian APT 33 infrastructure to attack dozens of organizations while posing as Iran.

While current focus is rightfully on Iran, our long-term security posture requires us to take a step back and ask ourselves *why* we are fearful of a threat from a nation state not considered our peer. The answer partly lies in the fact that despite more than a decades' worth of warnings, we know that critical American infrastructure in both the public and private sectors remains vulnerable to attack due to our continued failure to prioritize cybersecurity.

In the words of ICIT Fellow and Cymatic Chief Security & Trust Officer, Malcolm Harkins, "The only place where success comes before work is in the dictionary, and we haven't done the work to not be vulnerable."

As tensions simmer and the US prepares for impending digital conflict, it is vital that short-term offensive and defensive decisions be made based on research and fact-based analysis. This approach will improve the private and public sectors' ability to defend against attacks and result in our government making firm, yet responsible, decisions to defend our country, troops, citizens, and allies.

Simultaneously, we must also use this opportunity to reset our understanding of global conflict and make the cultural, policy, and digital changes necessary to reduce our national risk posture. Doing so will ensure future incidents, like our current situation with Iran, will not result in a national panic regarding our cybersecurity.

How A Lack of Prioritization Led to National Panic

When responding to the rampant fear of cyber retaliation from Iran, it is arguably as important to focus on answering the question “How did we get here?” as “What should we do?”

The discourse surrounding the possibility of an escalating physical confrontation with Iran was never centered on how prepared we were to defend ourselves, but the human, financial, and geopolitical cost of doing so. This remains in stark contrast to the initial and ongoing discussions regarding the threat of cyber attacks, which paint a picture of almost inevitable success for Iran.

One reason for this different reaction is that Americans are confident in our conventional offensive and defensive armed forces. However, this level of confidence does not extend to how the government and private sector have prioritized cybersecurity and decreasing digital risk.

Imagine if our nation’s leaders in congress, federal agencies, and businesses had heeded the warnings of technology experts over the past decade and built resilient systems, devices, and operational technology. Today, we would have a climate where government and private sector organizations were vigilant, but not scrambling to implement known policies and technologies against an established threat.

We must capitalize on the current focus on cybersecurity and digital threats to demand action from policy makers, business leaders, and technology manufacturers whose actions have marginalized information security. Failing to do so will result in continued uncertainty in the face of virtually every global conflict with even moderately capable nation states.

“The only place where success comes before work is in the dictionary, and we haven’t done the work to not be vulnerable.”

Malcolm Harkins, ICIT Fellow & Chief Security & Trust Officer, Cymatic

Iran is Capable of a Significant Cyber Conflict – But How Far Will They Go?

In April 2010, the Stuxnet worm, allegedly developed by the US and Israel, targeted Siemens industrial control systems (ICS) in developing nations such as Iran, Indonesia, and India. Iran’s nuclear infrastructure and oil and gas infrastructure were also targeted by the Duqu malware from 2009-2011 and the Flame malware in 2012. In response to these cyberattacks, Iran began rapidly developing its cyberwar infrastructure [1] [2].

Since then, the Iranian government has poured resources into developing its offensive capabilities, becoming a major player on the global digital warfare stage. In addition to

homegrown APT groups, its capabilities have expanded through the use of proxies, allies, and militia.

Of particular concern should be Iran's well documented attacks leveraging wiper malware, DDoS, and phishing campaigns, which we will detail in the next section of this report. Experts also fear that Iran is now prepared to use beachheads that were methodically planted throughout Industrial Control Systems (ICS) in critical-infrastructure organizations.

Our analysis of the size, scale, and targets of future attacks is refined when combined with our understanding of Iranian motivation, awareness of America's capabilities and willingness to act, and knowledge of international treaties and accepted rules of war concerning kinetic and non-kinetic cyberattacks.

[Iran's Understanding of US Military Capabilities Point to Cyber Retaliation](#)

It is undisputed that the US possesses the most powerful military in the world. The American government has the means to cripple Iranian infrastructure and its main source of revenue, its oil industry, through decisive military intervention. History has demonstrated that while Iran provokes through inflammatory rhetoric, armed attacks, and cyberwarfare, it does not want to incur a massive military response from the US. Iran understands that its military is inferior to the US militarily and will not act to provoke a direct military conflict. This is particularly true under the current administration which has been vocal about its views on the use of military force. This theory is supported by Iran's military response to the killing of General Soleimani, which, in the aftermath, was assessed as a calculated military response that balanced the regime's political imperative to respond with its desire to avoid additional US military intervention.

Despite the temporary de-escalation, experts believe that additional retaliation is likely so Iran can demonstrate its strength on the global stage, appease demands from hardline conservatives, and respond to regional voices calling for revenge. This need to respond while understanding the potential repercussions is why many experts believe that Iranian cyberattacks are forthcoming.

[International Law May Influence Iranian Response](#)

Given that Iran is unlikely to attempt further military attacks, the question is how to predict the targets of Iran's cyberattacks and how severe the outcomes will be. The next several sections of this paper explore these themes in depth based on an assessment of Iran's previous attacks. However, we must first examine how international law guides cyberwar and how that may influence Iran.

[The Tallinn Manual 2.0](#) is an academic, non-binding study on how international law applies to cyber conflicts and cyberwarfare. It was drafted by an international coalition of legal experts and NATO affiliates as a legal, technical, strategic, and operational assessment of cyber scenarios, with the aim of publishing a practical reference for Cyber Commands. While it is not a treaty, it does provide a reasonable estimation of the legal precedents and strategic implications that influence international kinetic and non-kinetic cyberattacks. In short, it may hold clues to how Iran could digitally respond to Soleimani's death through cyberattacks that border, but do not cross, the threshold of an act of war.

In the Tallinn Manual 2.0, international academic, legal, and military experts collaborated to draft 154 rules of cyberwarfare based on existing treaties, agreements, and case law precedent. Whereas the 2013 edition was limited in scope to international law on the use of force and international humanitarian laws, the second edition incorporated the application of peacetime international law since most cyber conflict occurs in times of peace. Furthermore, the manual found that while many cyber-actions do not cross the threshold of a kinetic response, the rules set forth imply that some financial, humanitarian, or geopolitical impacts may warrant a proportional response.

In [the context of The Tallinn Manual 2.0], and not counting the actions of rogue proxies or terrorist groups, it is reasonable to assume that Iran's attacks will be strategic in nature with a focus on causing disruption to the operations of organizations and minor cyber-kinetic outcomes as opposed to massive cyberattacks which cause extensive physical damage.

In this context, and not counting the actions of rogue proxies or terrorist groups, it is reasonable to assume that Iran's attacks will be strategic in nature with a focus on causing disruption to the operations of organizations and minor cyber-kinetic outcomes as opposed to massive cyberattacks which cause extensive physical damage. They are likely focused on degrading American critical infrastructure to demonstrate their strength and cause fear among the US population and allied societies. Analysts do not believe Iran has the resources and capabilities necessary to stage a major attack on large swaths of our critical infrastructure, nor is it beneficial to Iran to do so.

Iran's Modus Operandi: Disruptive Attacks

Iran is perhaps best known for using wiper malware to disrupt operations around the world. Wiper malware deletes all data stored on a device and requires system administrators to either reboot the device or restore it from backups.

Multiple Iran-based cyber groups with suspected ties to the government and the country's Islamic Revolutionary Guard Corps (IRGC) are believed to be capable of disrupting and damaging operations at US organizations. Top among them are APT33, one of the most active threat groups operating out of the Middle East; APT34 (aka OilRig/MUDDYWATER), and APT39, a relatively new group that targets companies in the technology, travel services, and telecommunications sectors [3]. Meanwhile, APT33 and APT34 are primarily focused on financial, energy, telecom, and SCADA/ICS [3].

Private sector companies responsible for critical infrastructure are often unaware that APTs might already be in their network. That poses a threat because the Iranian government and its hacker proxies are likely to prioritize targets where they have persistence access. Since 2012, the world has seen an increase in Iranian aggression leveraging this devastating attack vector:

- **Saudi Aramco:** In August 2012, Saudi Arabia's largest natural oil company, Saudi Aramco, suffered a cyberattack that leveraged the Shamoon wiper malware to damage approximately 30,000 computers. The attack on Saudi Aramco, which supplies 10% of the world's oil, failed to disrupt production, but remains one of the most destructive cyber strikes conducted against a single business.
- **Sands Casino:** On February 10, 2014, the Sands Casino suffered a widespread malware attack that wiped out 75% of the company's Vegas-based servers. Insiders estimate this cost the company more than \$40 million in equipment and data recovery alone. The attack seems to have been provoked by a speech where CEO Sheldon Adelson suggested detonating a nuclear bomb in the Nevada desert as a warning of what would happen if Tehran continued its nuclear program. In response, the attackers left a message on company servers, "Encouraging the use of Weapons of Mass Destruction, UNDER ANY CONDITION, is a Crime." The note was signed from the "Anti WMD Team." They also took down company websites, replacing them with a photograph of Adelson and Israeli Prime Minister Benjamin Netanyahu [4]. It is worth noting that the four-month window between the inciting incident and the Iranian retaliation indicates a measured patience.
- **Sapiem:** In 2018, the Italian oil company Saipem suffered a destructive cyberattack that leveraged the Shamoon malware. The attack was attributed to the Charming Kitten APT group, which has been linked to Iran in the past. As Saudi Aramco is a large Saipem customer, it is possible the attack was meant to disrupt Saudi Arabia's oil and gas supply chain [5].

Notable Iranian APTs

The table below offers a high-level summary of notable Iranian APTs:

Notable Iranian Threat Actors			
Common Name	Aliases	Target Sectors	Malware/ Toolkit
APT33	Magic Hound, Timberworm, MAGNALLIUM, Elfin, Refined Kitten, Holmium	Aviation, Aerospace, Defense, Energy	Shamoon, POWERTON, Ruler, PUPYRAT, POSHC2 (.NET backdoor), TURNEDUP, Autolt backdoor, Gpppassword, LaZagne, Quasar RAT, Remcos, SniffPass, DarkComet, Autolt FTP tool, .NET FTP tool, PowerShell downloader (registry.ps1), POSHC2 backdoor
APT34	Oilrig, COBALT GYPSY, Twisted Kitten, Crambus, ITG13, Chrysene, Helix Kitten, IRN2	Financial, Government, Energy, Chemical, Telecommunications	Helminth, ISMDoor, Clayslide, QUADAGENT, OopsIE, ALMA Communicator, customized Mimikatz, Invoke-Obfuscation, POWBAT, POWRUNER (PS Backdoor), BONDUPDATER, malicious RTF files CVE-2017-0199 and CVE-2017-11882, ELVENDOOR, PLink, PsExec, SSH Tunnels to Windows Servers, Webshells (TwoFace, DarkSeaGreenShell, LittleFace), ZeroCleare
APT35	Charming Kitten, Parastoo, iKittens, NEWSCASTER, NewsBeef, Phosphorus, Group 83	Academia, Government, Human Rights Group, Media	ALFA TEaM Shell, DROPSHOT, TURNEDUP, SHAPESHIFT, malicious HTA files, MacDownloader
APT39	Chafer, Cadelle, ITG07, Remix Kitten	Telecommunications, Travel	Remexi, PsExec, Mimikatz, Web Shells (aspx spy, b374k), nbtscan, plink, RemCom, VNC Bypass scanner, CoreSecurity tools, Impacket / Python exploits, NSSM, Remcom, HTTP Tunnel, Cadelspy, PLink, SSH Tunnels to Windows Servers
MuddyWater	TEMP.Zagros, Seedworm, SectorD02, Static Kitten, BlackWater	Government, Defense, Telecommunications, Oil, Information Technology	POWERSTATS, PoweMuddy, LaZagne, Crackmapexec

The following sections offer historical context for Iranian APT activity while focusing on Iran's most prolific threat group, APT33.

Operation Cleaver: Disassembled but Not Gone

In December 2014, Cylance, now owned by Blackberry, exposed the Iranian threat actor Tarh Andishan in the white paper describing their 2-year Operation Cleaver investigation. Tarh Andishan was likely developed in response to the Stuxnet, Duqu, and Flame campaigns. Iran could be demonstrating to global targets that it is a major cyber power, capable of competing with countries such as the United States, China, and Russia, on the global cyber landscape. Following the release of the report on Operation Cleaver, it is believed that Tarh Andishan's

infrastructure was abandoned and its capabilities and resources may have been reallocated into APT33, APT34, APT35, APT39, Muddy Water, and other Iranian nation-state APTs.

When operational, Tarh Andishan targeted government entities and critical infrastructure facilities in Canada, China, England, France, Germany, India, Israel, Kuwait, Mexico, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, United Arab Emirates, and the US. Specifically, Tarh Andishan targeted military installations, oil and gas facilities, energy facilities, utility facilities, transportation facilities, airlines, hospitals, telecommunication companies, technology firms, education and research institutions, aerospace and defense facilities, chemical companies, and governments. The expansive range of targets across the globe indicates that the Tarh Andishan campaign was likely a mechanism for gaining geopolitical leverage and establishing Iran as a cyber-power, perhaps with the intention of demonstrating that Iran could retaliate against any country that compromises its cybersecurity.

According to Cylance, Tarh Andishan's "Initial compromise techniques included web attacks, SQL injection, and creative deception-based attacks, all of which were previously implemented by China and Russia." Tarh Andishan did not appear to utilize zero-day exploits. SQL injection was made possible by attacking vulnerable applications that failed to sanitize SQL queries prior to passing them to a database. Later, Tarh Andishan began spear-phishing attacks, which involved sending specific victims an email with a malicious link. Via this method, Tarh Andishan compromised Microsoft Windows web servers that ran internet information services (IIS) Coldfusion, Apache servers with PHP, Microsoft Windows desktops, and Linux servers. The group also targeted popular network infrastructure such as Cisco VPNs, Cisco switches, and routers. Tarh Andishan's most utilized malware, TinyZBot, gathered information from infected systems and established backdoors for persistent access.

APT33

APT33 is currently the most prolific Iranian threat actor due to the public cyber-kinetic impacts realized from its disruptionware attacks. Though the group has only been operating in its current form since 2015, it is feasible that an early iteration of the state-sponsored threat launched the 2012 Disttrack attack against Saudi Aramco. APT33 engages in intellectual property theft, state sponsored espionage, and destructive attacks. For APT33, capturing lucrative information, such as defense intellectual property or insider data on the oil market, is just as valuable as the destructive attacks it conducts to send geopolitical messages.

This Iranian group currently focuses on exploiting vulnerabilities in ICS by leveraging the Shamoon 2.0 malware. In past attacks, the APT has compromised organizations through phishing campaigns and password-spraying attacks, where an adversary attempts to gain unauthorized access to a network using a small number of commonly used, (often complex) passwords against a large number of accounts. This strategy bypasses traditional “lockout” safeguards by only generating a handful of failed attempts per account. Microsoft asserts that APT33 recently became more focused, significantly narrowing its password spraying to around 2,000 organizations per month, while increasing the number of accounts targeted per organization almost tenfold [6] [7].

APT33 engages in intellectual property theft, state sponsored espionage, and destructive attacks.

A brief timeline of notable recent activity includes:

- From June to November 2018, APT33 sent out malicious phishing emails that weaponized .HTA attachments to deliver the POSHC2 or PUPYRAT malware to petrochemical, utility, insurance, education, and manufacturing organizations in North America, East Asia, and the Middle East. Following the initial compromise, the attackers leveraged POSHC2, POWERTON or RULER malware with compromised credentials to laterally navigate across the network and establish persistence.
- In mid-December 2018, APT33 or APT34 deployed the SHUTTERLITE malware in a disruptive attack against Sapiem, an oil company headquartered in Italy. The impacted company was a key supply chain partner of Saudi Arabian oil and gas companies.
- In June 2019, APT33 launched a phishing campaign that targeted governments and financial, retail, education, media, and entertainment sectors. The campaign leveraged job and financial lure emails with .HTA attachments to deliver the POWERTON and PUPYRAT malware.
- In June 2019, FireEye identified APT33 infrastructure that was used to deploy the RULER and POWERTON malware following password-spraying attacks.
- Around the same time, US CyberCom identified similar infrastructure being leveraged by APT33.
- In August 2019, APT33 used fake US defense contractor domains to deliver POSHC2 and KOADIC malware. The websites advertised career opportunities in Riyadh, Saudi Arabia, with specific US defense contractors.

Targeted Sectors

While opportunistic cyberattacks mean that virtually all public and private sector organizations must be on a heightened level of alert, a strategic assessment of Iran's motivations suggests certain sectors are particularly at risk.

Disruption to Energy, Water, and Critical Manufacturing

Iran has demonstrated the ability to successfully attack ICS and SCADA systems to cause disruption to critical infrastructure sectors, including energy and water services. Because cyber-kinetic attacks are more difficult to execute and are considered to be an escalation from purely cyber incidents, known past attacks of this nature from Iran have been limited.

For instance, according to Flashpoint Intelligence, the Iranian hacktivist group, SOBH Cyber Jihad, sent a message through another Iran-linked hacker outfit, Parastoo, promising to release technical information proving it was behind the 2013 breach of the New York Blind Brook Dam. A DHS investigation into the incident found that an intruder accessed and read files, including usernames and passwords, six times between August 22nd and September 27th, 2013. However, there is no indication that the attacker ever leveraged the credentials to manipulate the dam controls. While likely an opportunistic target, attackers compromise critical infrastructure, like dams, to signal to the United States that they possess the capabilities to attack meaningful critical infrastructure and, in some instances, to divert US resources to recovery and remediation of the assets.

Attacking the power and water supply also aligns with Iran's likely goal of striking fear into the hearts and minds of Americans, as opposed to causing major damage that could spark a major kinetic retaliation. Analysts also believe that, as part of its offensive strategy, Iran has been exploiting ICS vulnerabilities to gain access to critical infrastructure around the world, positioning itself for future attacks.

The Defense Industrial Base

Iran's rhetoric about its ability to inflict harm on US defense capabilities makes the defense industrial base (DIB) a prime symbolic target for cyberattacks. What better way for Iran to boast about a successful response than a massive disruption to the DIB?

While all members of the DIB should be concerned, compromising small and medium defense contractors who lack the resources and preparation to defend against cyberattacks could have a devastating impact on the DIB supply chain. Major disruption of the DIB supply chain would not only degrade our short and long-term capabilities, but also distress the US

What better way for Iran to boast about a successful response than a massive disruption to the DIB?

government, legislators, military personnel, and citizens as a whole. More importantly, attacks on private sector DIB organizations may not provoke an escalated response from US law enforcement or the military. Private US organizations lack the authority and often the capability to “hack back” an adversary; however, since attribution is difficult, especially during a cyberattack, it is unlikely that accurate and proportional retaliation would be possible. In short, attacks on vulnerable, private sector, small and medium DIB organizations may serve as a public demonstration of Iranian retaliation and cyber capabilities without intensifying the conflict on the geopolitical stage.

Financial Sector

In 2016, the US Justice Department unsealed the indictment against seven Iranians for launching DDoS attacks between December 2011 and September 2012 against US banks [8] [9] [10]. During this time, the hackers targeted 46 major financial institutions and corporations, including the Bank of America, Capital One, JPMorgan, Chase, PNC Banks, the New York Stock Exchange and Nasdaq. This left hundreds of thousands of customers unable to access their bank accounts and resulted in tens of millions of dollars being spent by victimized organizations to mitigate and neutralize the attacks. While a proxy group calling itself the Izz ad-Din al-Qassam Cyber Fighters repeatedly claimed credit for the attacks, the more likely motivation for the campaign was geopolitical [8].

The actual threat actors allegedly worked on behalf of the Iranian government, including the IRGC. Since General Soleimani was a ranking officer in the IRGC, it is reasonable to suspect that a sanctioned or unsanctioned retaliation for his death may occur with Iranian actors launching cyberattacks intended to sabotage American financial institutions or undermine the integrity of fair competition on the free market [8]. In fact, 85% of respondents to the Washington Post Cybersecurity 202 survey believe that Iran will launch retaliatory attacks against oil refineries, financial institutions, and other US targets within the next few months [11].

The Financial Services Information Sharing and Analysis Center, which gathers cyberattack reports from thousands of US banks, encouraged its members to stay vigilant even as it continues to closely monitor recent geopolitical developments. After all, what better symbolic revenge could Iran achieve than to go after the US economy? By targeting a US financial institution, Iranian hackers could inflict a substantial impact that may not warrant a military response [12].

Academia

In March 2018, the US Justice Department indicted nine Iranian actors associated with the Mabna Institute for conducting a massive cyber-theft campaign on behalf of the IRGC. The

thefts targeted academic and intellectual property and email account credentials. According to the indictment, the campaign targeted:

- 144 US universities
- 176 universities in 21 foreign countries
- 47 domestic and foreign private sector companies
- The US Department of Labor
- The Federal Energy Regulatory Commission
- The states of Hawaii and Indiana
- The United Nations, specifically the United Nations Children's Fund [10]

With this precedent, it is possible that US academic institutions could be targeted in retaliation for Soleimani's death, particularly those that engage in sensitive research for the government and defense sectors. Another potential risk is from hacktivists who want to escalate the conflict by targeting universities in campaigns designed to implicate Iranian students in the US. In doing so, xenophobic rhetoric may be escalated, encouraging the American public to support further conflict with Iran.

The Healthcare Sector

The healthcare sector was a prime target for the last Iran-based malware campaign, SamSam, which claimed multiple victims including Allscripts, Labcorp, and MedStar Health. Even before the current geopolitical tensions, the Cybersecurity and Infrastructure Security Agency Director Christopher Krebs warned the health sector:

Iranian regime actors and proxies are increasingly using destructive wiper attacks, looking to do much more than just steal data and money. These efforts are often enabled through common tactics like spear phishing, password spraying, and credential stuffing. What might start as an account compromise, where you think you might just lose data, can quickly become a situation where you've lost your whole network.

Wiper malware is arguably more devastating than ransomware. Where ransomware is designed to hold data hostage in exchange for financial gain, wiper malware is designed to completely destroy data and massively disrupt key business functions. According to a recent report from Carbon Black, about 45% of healthcare CISOs have already faced a wiper malware attack in the past year, with the majority of the sector seeing a steady increase in the sophistication of cyberattacks [13]. Additional attack vectors include tracking healthcare wearables, like Fitbits, to discern US military base information or attempting cyber-kinetic attacks against key US officials, similar to the threat against former Vice President Dick Cheney's heart implant [14] [15].

Increased Attacks from Other Enemies & and The Importance of Attribution

There is little question that Iran will launch cyberattacks against the US and its interests. However, it is not easy to assess how other enemies of the US and cunning cybercriminals alike will use the Iran/US conflict to launch their own attacks while obfuscating their true identity and masquerading as Iran. Similarly, Iran could launch attacks that leverage tactics and malware attributed to non-Iranian APTs as part of a layered campaign.

Nation States and Cybercriminals Posing as Iran

As recently as October 2019, there was direct evidence of nation states posing as Iran during cyberattacks. For instance, it is believed that the Russian APT Epic Turla, also known as Uroburos, Waterbug, Venomous Bear, Snake, or SnakeNet, had coopted infrastructure linked to the Iranian APT group APT34 which many security experts believe is backed by the Iranian government. Historically, APT34 focused heavily on victims in the Middle East, although it has compromised organizations across the globe. Tools previously tied to APT34 include Neuron, Nautilus, and Snake [16] [17]. This action enabled Epic Turla to confound attribution attempts and masquerade its espionage operations because they originated from known Iranian infrastructure.

It is not easy to assess how other enemies of the US and cunning cybercriminals alike will use the Iran/US conflict to launch their own attacks while obfuscating their true identity and masquerading as Iran.

Epic Turla is one of Russia's primary APT groups and its custom toolkit typically targets 32-bit and 64-bit Microsoft Windows systems that belong to governments, embassies, defense industries, pharmaceutical companies, research and education facilities, and other large companies. By masquerading as the Iranian APT34, Russia could conduct cyberespionage under the cover of the ongoing geopolitical conflict.

US intelligence agencies are almost certainly focused on this scenario being replicated by peer nation states, like Russia and China, and hail-mary threat actors with a fewer capabilities, like North Korea. They will likely be motivated to escalate the Iran/US conflict so they can take advantage of the ensuing crisis to further their geopolitical standing by degrading critical American infrastructure, stealing intellectual property, or disrupting the sectors driving our economy.

Iran Posing as Other Bad Actors

Similarly, Iran may use this strategy to hide the full scope and scale of its cyber-operations against the US and its interests. This would give Iran the ability to publicly claim some

cyberattacks to show its citizens and the world its strength, while not being held definitively accountable for more destructive attacks that would otherwise evoke a proportional response. These attacks could take the form of cyberattacks on critical infrastructure, intellectual property theft, or the theft of sensitive materials from the US Government.

Information Warfare

Another major concern is the use of social media to spread misinformation that further polarizes Americans and motivates Iranian sympathizers to act. We have already seen doctored images of Obama shaking hands with Iranian President Hassan Rouhani, which were retweeted by at least one member of congress. The image of Mr. Obama was actually taken from a 2011 event during which he was actually shaking hands with Indian Prime Minister Manmohan Singh in front of the Indian flag [18].

Figure 1: Side-by-Side Comparison of 2011 Doctored Image Used to Foster Controversy with Iran



In 2011, a picture of President Obama with Indian Prime Minister Manmohan Singh was used to create a false image of President Obama with Iranian President Hassan Rouhani. Viral socialization of the altered image spread as far as the US Congress, inciting controversy and conspiracies on the Internet. The public is susceptible to similar operations that may arise in retaliation to Soleimani's death.

In response to the death of Soleimani, a massive increase in the use of the hashtag #HardRevenge was observed [19]. Most of the tweets with the hashtag spread the same images of Soleimani, often shown in a military uniform in front of a flag, or alongside Iran's Supreme Leader, Ayatollah Khamenei. It was not immediately clear whether the accounts were controlled by real people or automated bots, but they tweeted in a variety of languages, including English, Arabic, and Farsi, to follower counts ranging from one or two to more than 3,500. Many of the accounts were created recently, as tension between the US and Iran grew.

Often, they used Soleimani's image as their profile picture, while some spread pictures of US military personnel with targets on their faces. Other posts included vivid depictions of mutilated bodies, with users claiming, without evidence, the images were of Soleimani's remains [19].

The Iranian government may also leverage information warfare against its own people, using the current conflict with the US to gain favor with a population who is largely dissatisfied with the ruling class. Between January 2018 and October 2019, there were over 4200 protests across Iran fueled by anger at the government's economic policies, opposition to the theocratic regime, and social and environmental issues. Manipulating facts and socializing false narratives about the US could direct anger away from the regime and toward a common cause. Following Iran's attack on a US base in Iraq, a disinformation campaign emerged that exaggerated US casualties and falsely claimed that US forces were withdrawing from Kuwait.

Mitigating Risk from Iranian Cyber Aggression

It is vital that private organizations and government entities recognize the urgency of the Iranian threat and immediately act to improve their resiliency. These measures should include:

Monitor for the Common Stages of Iranian APT Campaigns

At-risk organizations should prioritize detecting the initial stages of intrusions and implement ways to mitigate attacks by the following previously observed Iranian techniques:

- Password spraying
- VPN vulnerability
- RULER and exploiting CVE-2017-11774
- DNS Hijacking
- Spear phishing
- Malware sent via social media platforms

Immediate Cybersecurity Awareness Training for All Personnel

Organizations should leverage the mainstream media's focus on the potential of retaliatory Iranian cyberattacks to engage their board of directors, company executives, and non-manager personnel on cyber hygiene and cyber awareness. At the board level, this should include articulating the threat to the organization and asking for resources to mitigate the risk. Additionally, company executives should be briefed on the threat, understand the need for resources, and reminded that the cybersecurity culture of organizations starts at the top. Executives must hold themselves accountable to the same best practices expected of others in their organization and should send statements to their teams stating as much.

Company-wide training programs should also be revisited, or developed, to ensure that all personnel, regardless of position in the company, are reminded of the critical role they play in defending against cyber threats. These conversations should focus on phishing and insider threats, including phishing exercises that find and remediate poor habits.

Disaster Recovery Wargames

Organizations who do not regularly conduct disaster recovery wargames must develop and execute such programs. Those who do should conduct emergency exercises to refresh personnel on how to respond if an attack occurs.

Redundancy & Continuity of Operations

Given Iran's notoriety for using wiper malware and the threat of Iranian or other adversarial use of disruptionware, including ransomware, organizations should ensure their redundancy and continuity of operation programs (COOP) are being implemented and adhered to across the company. This includes identifying the most valuable assets in the organization, backing-up systems and data, and ensuring that systems are not unnecessarily exposed to opportunistic attacks via open ports or unsecured connections. As part of the COOP, organizations should identify the proper law enforcement to notify, have an incident response team, and acquire cyber insurance in the event of a cyberattack. Once a COOP plan is in place, organizations should implement policies to periodically revisit the plan, including checking that back-up systems are working properly.

Assess the Security Posture & Prioritize Remediation

The overall security posture of an organization depends on its sector, network architecture, and the cybersecurity tools and frameworks implemented across the organization. In a heightened state of alert, organizations should assess their security posture, identify weaknesses, prioritize according to risk-impact to the business, and act to mitigate threats based on priority. Activities could include:

- Threat hunting
- Penetration testing
- Third-party contractor access
- Credential management
- Segmentation of data and networks

Practice Long-Term Vigilance

The response from Iran could be immediate, they could wait for months, or it could be a combination of the two. While international conflict with other nations is never desirable, the current climate creates an opportunity for cybersecurity and risk leaders to develop and

propose programs for both immediate and long-term vigilance against the threat from Iran and other nation states.

Basic Cyber Hygiene

Most organizations still fail to practice basic cyber hygiene and ignore risk management best practices, both of which dramatically increase their vulnerability. Some areas of focus include:

- Disabling unnecessary ports and protocols
- Securing necessary ports and protocols through layers of technical controls that mitigate malicious traffic
- Logging and limiting all attempts to access Internet-facing portals
- Enhance monitoring of network and email traffic to reduce the risk of phishing
- Identifying data exfiltration and other anomalous network behavior
- Patching external facing equipment to prevent network compromise through exploitation of a known or zero-day vulnerability.
- Logging and limiting usage of PowerShell to detect and prevent adversaries from executing commands or laterally navigating further into the network.
- Implementing multi-factor authentication (MFA)
- Implementing least-privilege access for VPN, public-facing applications, and user accounts
- Enforcing password complexity requirements
- Auditing accounts and mailboxes to ensure that best practices are followed and legacy single-factor authentications are disabled
- Investigating anomalous behavior such as attempts at authentication, privilege escalation, or lateral movement

Conclusion

Iran unquestionably poses a threat to public and private sector organizations, and the US should sound the alarm, increase vigilance, and implement appropriate controls and layered security strategies. However, the fear of cyber retaliation from Iran is a reminder that every major conflict in the modern age will likely consist of the threat of conventional weapons and cyberwarfare.

Despite years of warning, many US organizations have failed to modernize their systems, adopt layered security controls, or build devices and applications that are secure-by-design. As a result, American critical infrastructure is vulnerable to retaliatory campaigns, the machinations of opportunistic attackers, and false-flag operations of enemy nation-states. To change this paradigm, we must use this experience to change our culture to one that prioritizes security and takes the necessary steps to truly mitigate risk.

Sources

- [1] "OPERATION CLEAVER", Cylance.com, 2014. [Online]. Available: https://www.cylance.com/content/dam/cylance/pdfs/reports/Cylance_Operation_Cleaver_Report.pdf. [Accessed: 29- Jan- 2020].
- [2] R. Lemos, "Disclosure Does Little to Dissuade Cyber Spies", Dark Reading, 2019. [Online]. Available: <https://www.darkreading.com/threat-intelligence/disclosure-does-little-to-dissuade-cyber-spies/d/d-id/1336273>. [Accessed: 29- Jan- 2020].
- [3] J. Vijayan, "DHS Warns of Potential Iranian Cyberattacks", Dark Reading, 2020. [Online]. Available: <https://www.darkreading.com/attacks-breaches/dhs-warns-of-potential-iranian-cyberattacks/d/d-id/1336741>. [Accessed: 29- Jan- 2020].
- [4] B. Elgin, "Now at the Sands Casino: An Iranian Hacker in Every Server", Bloomberg, 2020. [Online]. Available: <https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas>. [Accessed: 29- Jan- 2020].
- [5] L. Newman, "The Iran Hacks Cybersecurity Experts Feared May Be Here", Wired, 2018. [Online]. Available: <https://www.wired.com/story/iran-hacks-nuclear-deal-shamoon-charming-kitten/>. [Accessed: 29- Jan- 2020].
- [6] A. Greenberg, "Iran's APT33 Hackers Are Targeting Industrial Control Systems", Wired, 2019. [Online]. Available: <https://www.wired.com/story/iran-apt33-industrial-control-systems/>. [Accessed: 29- Jan- 2020].
- [7] A. Greenberg, "Iranian Hackers Launch a New US Campaign as Tensions Mount", Wired, 2019. [Online]. Available: <https://www.wired.com/story/iran-hackers-us-phishing-tensions/>. [Accessed: 29- Jan- 2020].
- [8] E. Chabrow, "7 Iranians Indicted for DDoS Attacks Against U.S. Banks", Bankinfosecurity.com, 2016. [Online]. Available: <https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989>. [Accessed: 29- Jan- 2020].
- [9] "Press Release - January 4, 2020: Department of Financial Services Issues Alert to Regulated Entities Concerning Heightened Risk of Cyber Attacks", Department of Financial Services, 2020. [Online]. Available: https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202001041. [Accessed: 29- Jan- 2020].
- [10] "Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad | CISA", Us-cert.gov, 2020. [Online]. Available: <https://www.us-cert.gov/ncas/alerts/aa20-006a>. [Accessed: 29- Jan- 2020].
- [11] J. Marks, "The Cybersecurity 202: Get ready for serious cyberattacks from Iran, experts say", The Washington Post, 2020. [Online]. Available:

<https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/01/13/the-cybersecurity-202-get-ready-for-serious-cyberattacks-from-iran-experts-say/5e1b7ef288e0fa2262dcbc70/>. [Accessed: 29- Jan- 2020].

[12] P. Crosman, "Should banks expect cyberattacks from Iran?", American Banker, 2020. [Online]. Available: <https://www.americanbanker.com/news/should-banks-expect-cyberattacks-from-iran>. [Accessed: 29- Jan- 2020].

[13] J. Davis, "DHS Warns Iran Hackers Targeting US with Data Wiper Cyberattacks", HealthITSecurity, 2019. [Online]. Available: <https://healthitsecurity.com/news/dhs-warns-iran-hackers-targeting-us-with-data-wiper-cyberattacks>. [Accessed: 29- Jan- 2020].

[14] B. Joshua, "US military reviewing security practices after fitness app reveals sensitive info", CNN, 2018. [Online]. Available: <https://www.cnn.com/2018/01/28/politics/strava-military-bases-location/index.html>. [Accessed: 29- Jan- 2020].

[15] A. Peterson, "Yes, terrorists could have hacked Dick Cheney's heart", The Washington Post, 2013. [Online]. Available: <https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheney-s-heart/>. [Accessed: 29- Jan- 2020].

[16] M. Schwartz, "Russian Hackers Coopted Iranian APT Group's Infrastructure", Bankinfosecurity.com, 2019. [Online]. Available: <https://www.bankinfosecurity.com/russians-hackers-coopted-iranian-apt-attack-infrastructure-a-13275>. [Accessed: 29- Jan- 2020].

[17] "Advisory: Turla group exploits Iranian APT to expand coverage of victims", Ncsc.gov.uk, 2019. [Online]. Available: <https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims>. [Accessed: 29- Jan- 2020].

[18] J. Freiman, "Republican congressman shares fake photo of Obama with Iranian president on Twitter", Cbsnews.com, 2020. [Online]. Available: <https://www.cbsnews.com/news/paul-gosar-twitter-republican-congressman-shares-fake-photo-of-barack-obama-with-iranian-president-rouhani-2020-01-06/>. [Accessed: 29- Jan- 2020].

[19] J. Stone and J. Stone, "Pro-Soleimani messaging immediately floods Twitter following general's death in drone strike - CyberScoop", CyberScoop, 2020. [Online]. Available: <https://www.cyberscoop.com/soleimani-twitter-revenge-campaign-disinformation/>. [Accessed: 29- Jan- 2020].