Alyssa Rose

COMP-116: Computer System Security

13-December-2019

Starting from Stuxnet: The Development of the US-Iranian Cyberwar

Iran and the United States have been engaged in a cyberwar beginning with the release of Stuxnet in 2010, a worm written by the United States and Israel targeting the Natanz nuclear plant in Iran. Attacks on the Iranian side have been led mainly by APT33, a prominent Iranian cyber fighter group going by a multitude of aliases, while the United States' strikes have acted as retaliations against Iranian aggression as a means of committing damage without human casualty. The attacks by APT33 have been propelled mainly by password spraying and spear phishing, which have allowed them to infect target systems with malware such as SHAPESHIFT and backdoors like TURNEDUP. As tension continues to escalate between the United States and Iran, there has been a drastic increase in such spear phishing and password spraying attacks by Iran, indicating that the groundwork for another Shamoon level attack is being formed. Analysis of this conflict allows for greater understanding of warfare in the digital era, and the cyber tactics employed by both sides whether they be classic or novel Black Hat methods.

Tension between the United States and Iran has manifested itself countless times in the forms of orchestration of coups ("US-Iran Relations: A Brief History"), hostage situations, and the shooting down of planes and drones. However, the recent strained relationship between Iran and the United

States has yet to form into a full-scale declaration of war, or at least one that is guided by the traditional rules of engagement. Under the surface, a cyberwar has been thriving since it was first waged in 2010 upon the release of Stuxnet (Zetter). The first of its kind, the unraveling and formation of this conflict lays the foundation for how cyberwarfare is enacted. Unbeknownst to most and unclear to many, there are few restrictions to the retailiations of the two forces, and the attacks evolve at a rate faster than any wartime tactics and line of defenses. This paper will delve into the technical and political repercussions of the US-Iranian cyberwar, including an analysis of Stuxnet (the first digital weapon that informally declared war), other cyber tactics used, and what it means for the future of wartime politics.

Analysis of this conflict is crucial to the general cybersecurity and political communities for two reasons: first and foremost, this conflict is establishing the foundation for a new form of warfare. The consequences of such cyberattacks do not manifest themselves in the standard tangible forms of most traditional war time offenses, nor is attribution entirely possible. This has led to two results; the conflict is largely unbeknownst to the general public and there are zero guidelines for rules of engagement. Thus, the tactics and attacks used by the United States and Iran are limited moreso to the technical capabilities of each respective force, and less to the military budgets of each which has traditionally been the predictor of the 'winner' of the war. Secondly, the concentration of resources into the offenses and defenses results in the side effect of progress in the field. Development of new malware and attacks will eventually find their way to the greater community (as seen in the ease of spread that Stuxnet thrived on), which provides new material and concepts for use and adaptation by Black Hat hackers. Equally so, the line of defense against such cyber attacks will attempt to linearly or exponentially scale. This provides an environment for innovation in proactive security, which becomes more necessary as the creativity of

the attacks grow. Consequently, the success of the war efforts are contingent on quality, rather than quantity.

Beginning in January of 2010, the nuclear plant located in Natanz, Iran began to experience unprecedented failure of centrifuges responsible for the enrichment of uranium gas as the centrifuges would spin too quickly, resulting in self destruction. As centrifuge failure occurred, the source of the issue was finally discovered by security specialists in Belarus; malware that targeted supervisory control and data acquisition (SCADA) systems that were manufactured by Siemens (specifically, Siemens Step7 software). The malware was able to gain control of the machinery, allowing for control of the industrial program logic controllers. Despite the antiquity of the attack, Stuxnet was the unofficial declaration of cyberwar between the US and Iran, a conflict that has not slowed since.

After the launch of Stuxnet, Iranian forces began their own attacks, starting with 'Operation Ahabil' led by members of Izz Ad-Din Al Qassam (also known as the Qassam Cyber Fighters) that targeted various American banks through use of distributed denial of service (DDoS) attacks. These attacks were standard DDoS attacks with the extra exploitation of flooding the banks websites with encryption requests (Perlroth, and Hardy).

Despite the continuing issue of attribution, the main perpetrator on the Iranian side is a group known as APT33 (also known as Refined Kitten, Elfin, Holmium, Magnallium) that has been active since 2013. The focus of APT33 resides mainly in the aviation and energy sectors ("APT33, Elfin") with spear phishing attacks targeting employees in the aviation sector in 2016. The spear phishing was conducted via links to malicious HTML application files (.hta) (O'Leary et al.) that allowed for the downloading of an APT33 backdoor. Such spear phishing attacks again appeared in June of 2019,

targeting US national labs and the Department of Energy (Greenberg). Additionally, APT33 has continued to use password-spraying techniques throughout all of 2019, targeting manufacturers, suppliers, and maintainers of industrial control systems as reported by Microsoft (Greenberg). In October of 2019, the Microsoft Threat Intelligence Center (MSTIC) reported attempts to access and attack around 241 email accounts associated with the U.S. presidential campaign, government officials, journalists, and Iranian citizens living outside of Iran (Burt). Although the attacks were attributed to an unknown group (dubbed 'Phosphorus' by Microsoft) originating from Iran, APT33 has been considered the likeliest actor.

Despite the seemingly low scale attacks, Iranian cyber forces have been responsible for the installation of malware and backdoors, including the infamous Shamoon worm that resulted in thousands of computers having their master boot record and data wiped. Shamoon was originally launched in 2016, via means of spear phishing emails that included a document with a malicious macro that when executed, allowed for access and control through a remote PowerShell (Albano, and Kessem). Although APT33 has not been directly tied to Shamoon, APT33 has employed the use of DROPSHOT (a dropper) that is linked to SHAPESHIFT (also referred to as StoneDrill), malware capable of wiping disks and deleting large volumes of files, which resembles closely the most recent versions of Shamoon. However, DROPSHOT is well above Shamoon in sophistication as it uses external scripts for self deletion and memory injection for the deployment (O'Leary et al.). DROPSHOT has also been used for the installation of TURNEDUP, a backdoor that was used for an array of attacks that were largely prominent in 2017.

As such, the increase in password spraying and spear phishing attempts in October and November of 2019 indicate that the groundwork for a larger scale attack, most likely targeting industrial

control systems in power grids and manufacturing facilities, is possible. Such attacks would serve the purpose of retaliation for the withdrawal of the 2015 nuclear deal by the Trump administration, and blame that was placed on the Iranian government for the drone strikes on one of the largest oil processing facilities in September of 2019. After the attack in September, the United States launched a cyber strike on Iran, a strike that supposedly affected physical hardware (Ali, and Stewart) and demonstrates the United States' willingness to engage in such a cyberwar when physical attacks would prove to be too risky, choosing to engage in damages without human casualty. As such attacks become more commonplace as the tension between the United States and Iran increases, the analysis and consideration of various defenses is crucial.

As the threat of another Shamoon level attack looms from Iranian forces, analysis of the first deployment of Shamoon provides insight into possible defensive measures that may be enacted by the United States. Foremost, password spraying efforts can be mitigated with stronger passwords, requirements that could be enforced by Microsoft and the IT departments of the various US national labs, manufacturing facilities, and aerospace/energy sector companies. DROPSHOT's deployment was also contingent on the success of spear phishing that allowed for the downloading of documents with a malicious macro. In APT33's earliest attacks employing distributed denial of service (DDoS) methods, rate limiting and locating data centers on different networks may have mitigated the effects of such attacks ("What Is A DDOS Attack & How To Protect Your Site Against One") . Overall, educating workers at targeted organizations (and the general public) on not downloading files from unknown sources (preventing against spear phishing) and the importance of complex passwords would have easily

stopped such attacks as in Stuxnet, Shamoon, DROPSHOT/SHAPESHIFT, where the weakest link in the attack was human error.

The cyber conflict between the United States and Iran has shown the possibility that war may be waged in the digital space with consequences manifesting in physical damage to systems and infrastructures. The tactics used by each side are well worn, and showcase the power of exploitation of common vulnerabilities and weaknesses. Common attack methods have continued to evolve into more sophisticated strikes including SHAPESHIFT malware and the TURNEDUP backdoor as the conflict draws on. Such a conflict presents a case study of what warfare may look like in the future, the limits of cyber attacks damage in the physical world, the dangers of human error, and the consequences of a lack of ubiquitous cybersecurity education. Such warfare provides the opportunity for all actors, regardless of military size or budget, to engage in damage to the computational and infrastructural resources of the enemy, placing the opportunity for winning the conflict more so upon the creativity that has allowed the Black Hat community to thrive than budget or military size.

References

Ackerman, Geoff et al. "OVERRULED: Containing A Potentially Destructive Adversary". *Fireeye*, 2018,https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html. Accessed 13 Dec 2019.

Albano, Kevin, and Limor Kessem. "The Full Shamoon: How The Devastating Malware Was Inserted Into Networks". *Security Intelligence*, 2017, https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/.

Ali, Idrees, and Phil Stewart. "Exclusive: U.S. Carried Out Secret Cyber Strike On Iran In Wake Of Saudi Oil Attack: Officials". Reuters, 2019, https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK.

"APT33 (Threat Actor)". Malpedia.Caad.Fkie.Fraunhofer.De, https://malpedia.caad.fkie.fraunhofer.de/actor/apt33.

"APT33, Elfin | MITRE ATT&CK™". Attack.Mitre.Org, https://attack.mitre.org/groups/G0064/.

Beek, Christiaan. "TURNEDUP". *Attack.Mitre.Org*, https://attack.mitre.org/software/S0199/.

Brewster, Thomas. "Warnings As Destructive 'Shamoon' Cyber Attacks Hit Middle East Energy Industry". *Forbes.Com*, 2018, https://www.forbes.com/sites/thomasbrewster/2018/12/13/warnings-as-destructive-shamoon-cyber-attacks-hit-middle-east-energy-industry/.

Burt, Tom. "Recent Cyberattacks Require Us All To Be Vigilant". Microsoft On The Issues, 2019, https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/.

Curley, Robert et al. "Stuxnet | Computer Worm". Encyclopedia Britannica, https://www.britannica.com/technology/Stuxnet.

Doffman, Zak. "Secret Iranian Network Behind 'Aggressive' U.S. Cyberattacks Exposed In New Report". Forbes.Com, 2019, https://www.forbes.com/sites/zakdoffman/2019/11/14/secret-iranian-network-behind-aggressive-us-cyberattacks-exposed-in-new-report/#7fd6b84f579c.

Gates, Guilbert. "How A Secret Cyberwar Program Worked". Archive.Nytimes.Com, https://archive.nytimes.com/www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html.

Gilchrist, Karen. "US-Iran Cyber Strike Marks a Military 'Game Changer,' Says Tech Expert." *CNBC*, CNBC, 2 July 2019, www.cnbc.com/2019/07/02/us-iran-cyber-strike-marks-a-military-game-changer-says-tech-expert.html.

Greenberg, Andy. "New Group Of Iranian Hackers Linked To Destructive Malware". Wired, 2017, https://www.wired.com/story/iran-hackers-apt33/.

Greenberg, Andy. "Iranian Hackers Launch A New US Campaign As Tensions Mount". Wired, 2019, https://www.wired.com/story/iran-hackers-us-phishing-tensions/.

Greenberg, Andy. "Iran'S APT33 Hackers Are Targeting Industrial Control Systems". *Wired*, 2019, https://www.wired.com/story/iran-apt33-industrial-control-systems/.

Groll, Elias. "The U.S.-Iran Standoff Is Militarizing Cyberspace". *Foreign Policy*, 2019, https://foreignpolicy.com/2019/09/27/the-u-s-iran-standoff-is-militarizing-cyberspace/.

Hennigan, W.J. "The U.S. and Iran Are Already at War Online." *Time*, Time, 27 June 2019, time.com/5615628/iran-united-states-trump-cyberspace-digital-war/.

Holloway, Michael. "Stuxnet Worm Attack On Iranian Nuclear Facilities". Large.Stanford.Edu, 2015, http://large.stanford.edu/courses/2015/ph241/holloway1/.

"Iran: Target And Perpetrator - Iran'S Cyber Threat: Espionage, Sabotage, And Revenge". Carnegie Endowment For International Peace, 2018, https://carnegieendowment.org/2018/01/04/iran-target-and-perpetrator-pub-75139.

"Iranian Hackers Escalate Cyber Campaign against US amid Rising Tensions." *CNBC*, CNBC, 22 June 2019, www.cnbc.com/2019/06/22/iranian-hackers-escalate-cyber-campaign-against-us-amid-rising-tensions.html.

Kartch, Rachel. "Distributed Denial Of Service Attacks: Four Best Practices For Prevention And Response". *Insights.Sei.Cmu.Edu*, 2016, https://insights.sei.cmu.edu/sei_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html.

Kundaliya, Dev. "Iran-Linked APT 'Charming Kitten' Adds New Impersonation Tactics To Trick Potential Victims | Computing". Http://Www.Computing.Co.Uk, 2019, https://www.computing.co.uk/ctg/news/3082586/iran-apt35-charming-kitten.

Lindsey, Nicole. “Cyber War Between Iran and United States Could Have Far-Reaching Implications.” *CPO Magazine*, 13 Oct. 2019, www.cpomagazine.com/cyber-security/cyber-war-between-iran-and-united-states-could-have-far-reaching-implications/.

Perlroth, Nicole, and Quentin Hardy. "Bank Hacking Was The Work Of Iranians, Officials Say". *Nytimes.Com*, 2013, https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

O'Flaherty, Kate. "Iranian Hackers Are Going After A Disturbing New Physical Target". Forbes.Com, 2019, https://www.forbes.com/sites/kateoflahertyuk/2019/11/21/iranian-hackers-could-be-going-after-a-disturbing-new-physical-target/#31fc67077d2a.

O'Leary, Jacqueline et al. "Insights Into Iranian Cyber Espionage: APT33 Targets Aerospace And Energy Sectors And Has Ties To Destructive Malware". *Fireeye*, 2017, https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html. Accessed 13 Dec 2019.

Sanger, David E. “U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam.” *The New York Times*, The New York Times, 24 Mar. 2016, www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html.

Wagtendonk, Anya van. “Trump Called off a Military Strike against Iran. The US Targeted Its Computer Systems Instead.” *Vox*, Vox, 23 June 2019, www.vox.com/2019/6/23/18714327/iran-us-donald-trump-cyberattack-drone-strike.

"US-Iran Relations: A Brief History". BBC News, 2019, https://www.bbc.com/news/world-middle-east-24316661.

"W32.Disttrack.B". *Symantec.Com*, 2016, https://www.symantec.com/security-center/writeup/2016-112300-5555-99.

"What Is A DDOS Attack & How To Protect Your Site Against One". *Amazon Web Services, Inc.*, https://aws.amazon.com/shield/ddos-attack-protection/.

Zetter, Kim. "An Unprecedented Look At Stuxnet, The World's First Digital Weapon". WIRED, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.