THE HISTORY AND IMPLICATIONS OF CYBERWARFARE FOR CORPORATIONS, GOVERNMENTS, PEOPLE, AND SOCIETY: CASE STUDIES EXAMINING HOW INDIVIDUALS CREATE VULNERABILITIES IN THE INFORMATION SECURITY FIELD

by

Levi David Milton

HONORS THESIS

Submitted to Texas State University
in partial fulfillment
of the requirements for
graduation in the Honors College
December 2022

Thesis Supervisor:

Zachary Kelley

Second Reader:

Joshua J. Daspit

TABLE OF CONTENTS

Abstract

Cybercrime has been in existence since computers came into our lives. As time passed, computers became more sophisticated, along with the criminals exploiting them. Cybercrime has become a reality that many businesses, governments, corporations, organizations, and individuals must face. However, how did we get to this point? This research investigates eight case studies that helped shape our world today, allowing the acceleration of cyberwarfare from nation-states like Iran, North Korea, Russia, and the United States. Each case study consists of an overview of what happened, the history of why it happened, the financial impact created, how the attackers orchestrated the attack, and how society can prevent such acts going forward. Billions of dollars lost, fake personas, false flags, election fraud, crime syndicates, and ulterior motives are all present in these case studies. Organizations can use the conclusions drawn from these case studies to help understand how to prevent such acts.

Introduction

Cybercrime and hacking were introduced into society with the invention of computers and the advancement of technological industries. Whether it be the Enigma machine during World War II (WWII) or nation-states attacking various financial and government sectors, cybercrime has existed for almost 100 years. Until recently, cyberwarfare did not appear too often, but the societal transition to an online world has opened many avenues for criminals to exploit. Individuals, groups, and nation-states are responsible for the proliferation of malware, ransomware, and cyberattacks worldwide. This study will review significant events that shaped the history of "hacking" and examine why the attack happened, the motive(s), and what allowed the attacks to occur. By studying the overall facilitation of these attacks, organizations can learn from them by connecting similarities noted by researchers and by identifying solutions to potentially prevent attacks from happening in the future. This study aims to present information on this crucial topic in a manner easily understandable by individuals with limited or no expertise in the area. Additionally, the study seeks to provide information that may help mitigate future attacks.

When shining a light on nation-states involved in cyberwarfare, it shines brightest on four countries of interest: Iran, North Korea, Russia, and the United States (US). Although there are other countries of interest, these are generally considered four significant players in cyberwarfare and are, thus, the focus of this study. To further understand why these nation-states use cyberwarfare, we must realize the history leading to such decisions. Therefore, this investigation examines cases in the four nation-states of

interest. In each case, information is presented on what occurred, the history of why the respective attack happened, the financial impacts, and how the attackers orchestrated the attack.

Section 1: Iran

The Beginning

Iran and the US have had quite a history of diplomacy. Most people agree that Iran and the US are opposites in the political spectrum and world politics. While this is true, it has not always been that way. From 1941-1979, Mohammad Reza Pahlavi, known as the Shah (which, in Farsi, translates to “the King”), governed the people of Iran. His rise to power comes from his father, Reza Shah Pahlavi, who was also the Shah from 1925-1941 but left the country due to the invasion of Iran in World War II. Shortly after, the US and the United Kingdom (UK) supported a coup d'état that overthrew the opposition party and reinstated his son as Shah and Supreme Leader of Iran [1].

The installation of the Shah is the beginning of a prosperous relationship between Iran and the US. The Shah ultimately had one goal: to make Iran a global power by investing billions into his country’s infrastructure, military, education, and industries. During this time, the average income of an Iranian citizen rose 431 times over previous numbers, paving the way for the country to grow to become a world power. Education was vital to his rule also, with the Shah developing numerous new schools and universities – that offered free food for students – and focusing on remote regions of Iran that had previously been in poverty. From 1967-1977, literacy rates went from 27% to 80%. Ultimately, his domestic policies on education improved the country’s literacy and allowed many Iranians to achieve a higher level of education [2].

The Shah bought billions of dollars of weapons using the country's vast oil resources to expand his military, which he believed was a method of preventing further military intervention in his country. Beginning in the 1960s, the Shah helped support the defense industries of the US, the UK, France, Italy, and Russia, although most were from the US [3].

The Shah was constantly making deals, and the US even validated the claims by praising him as a valuable customer, claiming the defense industry made over $1,000,000,000 in profit with over 1,400,000 person-years of employment. Iran's economic and military growth was due to its strong ties with the US, which consisted of billions of dollars of arms sales over the years [4]. In return for the US helping the Shah, he positioned Iran as the US's key ally in the Middle East. While this may have seemed like a genuine relationship between the two countries, the citizens of Iran did not feel the same.

In the late 1970s, citizens became upset with their leader due to rising tensions with the Shah's policies. During this time, the Shah developed chronic lymphocytic leukemia, which delayed his ambitions, political trips, and, ultimately, his career as a world leader. Under heavy medication, the Shah could not make critical decisions about Iran's ongoing protests and problems while being treated for his cancer at his extravagant Caspian Sea fortress. Eventually, his French doctors notified the government of France that he had cancer and was indeed dying, and the country of France relayed the message to the Americans [5].

While the Shah was indecisive, protests and civil unrest kept rising, and blame for the country's problems fell on the Shah. The Shah helped train Iran's military with the

assistance of the defense industry from several western countries since Iran's military was not well versed in handling civil unrest. On multiple occasions, the military opened fire into crowds of innocent people, the most prevalent being Black Friday when thousands of people gathered in Tehran's Jaleh Square for a religious protest. Eventually, the protesters were met with gunfire from the military, and many innocent people were killed or injured. Emerging from the ashes was the Shah's most prominent rival: Ayatollah Khomeini, who had questioned the Shah's rules and policies. The people of Iran dubbed this as "the point of no return;" a revolution was inevitable [6]. The Shah soon fled the country in exile, eventually being welcomed to America by President Jimmy Carter, who cited his medical situation as the main reason for his acceptance [7].

While the US and Iran had been close allies during the Shah's reign, the alliance was built on the premise of money and power. Using the fortune created from their vast oil reserves, combined with the power and reach of the US defense industry, Iran maintained an alliance with US interests in the Middle East. At the same time, the US would continue to sell billions of dollars in weapons to Iran. As one might guess, the public perception from the Iranians was very hostile toward this relationship. People did not like their country acting as a puppet for the Americans and thought the Shah was moving Iran in the wrong direction. At the same time, many other factors related to the dislike of the Shah's reign and his close ties with the US were instrumental to the regime's fall. The US had backed the coup d'état in 1953, provided billions of dollars in defense sales, admitted the Shah into the US after he had fled the country, and overall had different ideologies than the people of Iran, which led to a massive distrust with the US and the western world.

Iran's cyberwarfare sector started to develop in the 2000s, with the creation of the first well-known Iranian hacker group - Ashiyane Digital Security Team (ADST). Created by Behrooz Kamalian (known online as Behrooz_ice), also known as the 'father of Iranian hacking,' ADST attacks consisted of highly visible website defacements, most notably including NASA and Mossad websites [8]. When someone visits the site, instead of being greeted with a typical NASA or Mossad interface, the website shows pro-Iranian messages and support for the ADST. See Figure 1 for an example of these messages.

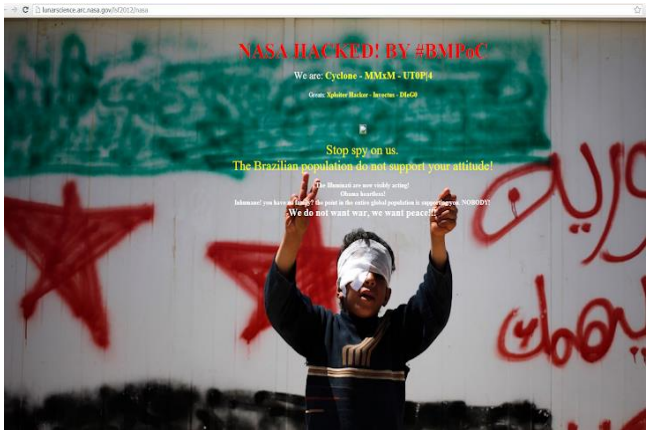

Figure 1 - ADST Defacement [9]

The home page of these websites was not affected, but specific pages were attacked. Examples of specific pages include:

https://event.arc.nasa.gov/sites/

https://kepler.nasa.gov/news/managerupdates/

https://lunarscience.arc.nasa.gov/lsf2012/nasa

https://planetaryprotection.nasa.gov/images/

https://academy.arc.nasa.gov/hi.html

https://astrobiology2.arc.nasa.gov/images/

https://virtual-institutes.arc.nasa.gov/images/

Ashiyane Digital Security Team also created a web forum where users, who consisted of Iranian citizens interested in hacking, could discuss various cybersecurity topics. It propelled the hacking community in Iran, offering a centralized place where users could come together for discussion and, most importantly, hack under its name, the Ashiyane Digital Security Team. With the implementation of this web forum, ADST quickly became one of Iran's top hacking groups. ADST even implemented a hacking school, the Ashiyane Digital Training Center, where it taught courses on hacking and security.

The Iranian Cyber Army came into existence around 2009. The Iranian Cyber Army was a more formal organization than ADST, mainly from being endorsed by the Islamic Revolutionary Guard Corps (IRGC). (For more detail on IRGC, refer to Appendix A.) In a quote from 2010, the commander-in-chief stated, “Today we take pride in our (Iranian) Cyber Army founded by us, which is the second strongest Cyber Army in the world [10].”

Evidence supports that both the ADST and the IRGC are related. When defacing websites, both groups posted word-for-word pro-Hezbollah messages (an Islamist political party and militant group). Additionally, while circumstantial, both groups originated from the same part of Iran. The origins of the two groups are most likely due to the idea that Ashiyane/ADST created the Iranian Cyber Army to conduct operations for the IRGC. The identical messages posted by ASDT, the IRGC, and both groups originating from the same area, make this connection feasible. Although ADST is not the only hacking organization in Iran, its primary organization can be traced back to what has grown into the cyberwarfare component of Iran. [10]

DigiNotar/Gmail Breach (2011)

Overview

In 2011, an Iranian citizen with the alias Alibo began to have trouble with his Gmail account. Whenever he attempted to log in, he received a security warning questioning the validity of the SSL certificate used to authenticate to the Gmail website. (See Appendix B for more information on how SSL certificates work.) Since Gmail was a reputable email service, Alibo always accepted this risk, assuming it was an error and not a security issue.

Alibo attempted to circumnavigate the problem at the time using a VPN (See Appendix C for information regarding VPNs), which allows users to mask their internet protocol (IP) address when browsing the internet. Despite its controversy with the Iranian government, which has a history of cracking down on VPNs, it seemed to fix the problem. He could finally access his Gmail without resolving the certification authentication issue. Using a VPN, he could use an IP address that originated outside Iran. When he turned the VPN off, the problem would resurface. Alibo concluded that the certificate issue only applied to users in Iran, although unsure why since Iran had not officially imposed any internet restrictions at the time. His next step was to post his problems to Google's online support forum. A couple of days later, he finally started to receive some answers.

Google released a public statement following up on the forum post that Alibdo created. To his surprise, Google stated that it had been the victim of an attack via a third-party program that used an elaborate SSL man-in-the-middle attack. (See Appendix D for information about man-in-the-middle attacks.) The attack allowed for the issuance of

false certificates by a compromised party and, in turn, allowed viewing unencrypted data from 300,000 Iranian Gmail accounts. This highly sophisticated attack was one of the government's first instances of mass surveillance using today's technology [10].

This affected many people and companies, and DigiNotar - the certificate company that was compromised to issue fake certificates - “voluntarily” declared bankruptcy. Additionally, the Dutch Government spent considerable resources assisting DigiNotar with its bankruptcy process and other related tasks [15].

History

To fully understand why someone would compromise a highly reputable company like DigiNotar in a case like this, one must understand the implications of the Srebrenica Genocide. Over 11 days in 1995, the Srebrenica Genocide resulted in more than 8,000 Bosnian men and children deaths. Bosnia is a melting pot of cultures, with a majority of the population being Muslim Bosniaks (44%) and also having Orthodox Serbs (31%) and Catholic Croats (17%) [16]. After the fall of Yugoslavia - the country that previously ruled this area - the people decided to hold a referendum for independence. The overall population supported this; thus, it went into effect despite solid opposition from the Orthodox Serbs.

Nonetheless, the Republic of Bosnia and Herzegovina - the newly formed independent country - was formally recognized by the United Nations (UN) and the European Union (EU) in the Spring of 1992 [17]. The Serbians were not happy about this, and they decided to retaliate. Bosnian Serb forces attacked the newly formed Republic of Bosnia to secure their territory so they could rule over their republic. Located in the middle of

their anticipated territory was a town called Srebrenica. This town was a strategic location for the Serbians, given that it was in the center of two parts of the envisioned Republic of Srpska. Serbian troops approached the city and demanded that the Bosnian Muslims surrender their weapons and leave within 24 hours. Some went, but most stayed to fight for their homeland. Srebrenica was surrounded by the Serbians, isolated from the outside. The Serbians proceeded to enter various neighborhoods and villages, usually killing the defenseless men, women, and children they stumbled across.

In April of 1993, the western world stepped in, with the first United Nations Protection Force troops arriving in Srebrenica, officially declaring the city a "safe zone." They ordered the Serbians to hand over their weapons and retreat far away from the town so they could not terrorize its citizens. Unfortunately, the Serbians did not listen. While there were a few years of peace after the UN arrived, the Serbians kept plotting for revenge. In 1994, the UN sent 600 Dutch troops to replace the Canadian troops stationed in Srebrenica. Less than a year later, the Dutch reported that Serbian forces controlled the territory surrounding Srebrenica, preventing outside access (even the UN's supply line could not reach the city). The Dutch troops alerted the UN of the situation, but the UN failed to act and provided no military or humanitarian assistance. By early 1995, the city had fallen into anarchy, with prostitution running rampant in the streets and minor skirmishes between civilians and Serbian troops happening on the outskirts of town. As time passed, soldiers went on leave for medical and personal reasons. They could not return due to the current situation in Srebrenica, dwindling the Dutch forces from 600 to 400. Also, due to the blockade by the Serbs, the citizens could not get any food, eventually leading to starvation. Citizens reported multiple deaths from starvation [19].

On July 11th, the situation started to turn for the worse, and the Serbians initiated their attack. With over 2,000 soldiers, the Serbians had the advantage, and the UN outposts began to fall. The attackers captured 30 Dutch soldiers and demanded that the UN stop air attacks on Serbian positions [18]. The UN agreed to their demands and stopped providing air support. The citizens of Srebrenica surrounded the UN base and pleaded for help, but soon the executions began, and it was chaos. Serbian soldiers randomly took people out of crowds and executed them without real organization. The Serbians eventually separated the men and women. They sent them off to another local town, but survivors reported that very few men had reached their destination, being killed by the Serbs with no intention of ever letting them live. By July 13, two days after the final attack, almost no males were left in Srebrenica [19].

The citizens of Srebrenica reported various war crimes committed by the Serbians (e.g., rape, killing of infants and pregnant women, and other gruesome crimes) as the remaining Dutch soldiers sat back and watched, with the Serbs outnumbering the Dutch troops. Independent journalists report that at least 8,000 unarmed civilians were murdered by the Serbs [20].

Overall, Iranians and the Muslim community blamed the outcome of the Srebrenica Genocide on the Dutch government, claiming they failed to recognize the situation and act accordingly. In 2002, the Dutch government accepted partial political responsibility for the events. Still, the people of Bosnia, Srebrenica, and neighboring countries were not happy with the Dutch government's response.

Impact

DigiNotar's parent company, VASCO Data Security (now formally OneSpan), is an international cybersecurity company based in the US with offices worldwide. They offer services such as identity verification and authentication, electronic signatures, fraud analysis, and mobile app security.

In January 2011, VASCO Data Security acquired DigiNotar for $12,900,000 [21]. About six months later, DigiNotar's systems were breached by an outside authority, issuing hundreds of fake certificates to websites worldwide. Shortly after the initial breach, its trust was stripped from them by the security community, and it was deemed untrustworthy. On Monday, September 19, 2011, they finally filed for bankruptcy. In VASCOs 8-K Filing to shareholders on Sept. 20, VASCO expected the following write-offs to be incurred [22]:

“As a result of these events (the ‘DigiNotar events’), VASCO expects to record impairment charges, write off net liabilities, record recoveries of contingent consideration, and record other bankruptcy-related expenses that, in total, range from approximately $3.3 million to $4.8 million. The estimated range of loss reflects the following estimates:

- The non-cash charge for the write-off of goodwill related to the purchase of DigiNotar of 2.9 million,
- The non-cash charge for the write-off of purchased intangible assets, net of amortization and related deferred tax liabilities, of DigiNotar of $1.5 million,

- A write-off of net assets (liabilities) of DigiNotar in a range of $0.1 million to $(0.9) million,
- A recovery from escrow of contingent consideration of $1.1 million, and
- Other bankruptcy-related costs range from approximately $0.9 million to $1.4 million."

The fall of DigiNotar did not affect the overall success of VASCO. While DigiNotar incurred millions of dollars in losses and reflected those losses in its tax deductions, VASCO Data Security still had a net profit of $2.2 million for the third quarter of 2011 [22] when it wrote off the items mentioned above. Unfortunately for VASCO, the lasting impact of DigiNotar did not end with a write-off for the 3rd quarter of 2011. While it continued to grow as a substantial international cyber-security business, it eventually rebranded in 2018, encompassing the new brand of "OneSpan." While it happened many years after the fall of DigiNotar, this is no coincidence considering the stain DigiNotar left on VASCO.

The Dutch Government also suffered an immense amount of embarrassment surrounding the hack of DigiNotar due to its extensive involvement in the company. The Dutch used their certificate authority services to assist with various government programs, like an authentication infrastructure (DigiD) and the government car registry (i.e., Netherlands Vehicle Authority). After the Dutch realized that the systems were compromised, they had to re-issue correct certificates to government websites after taking control of the operations of DigiNotar. Alongside this, the Minister of the Interior for the Netherlands also announced that the government could no longer guarantee the security of its websites

and urged the public not to log onto them until new certificates were obtained from other issuing authorities [23].

This attack ended up costing all parties involved tens of millions of dollars. VASCO bought DigiNotar for $12.9, and while it owned DigiNotar, unfortunately, DigiNotar had no significant income before the attack. Therefore, investigators can conservatively say that VASCO lost a total of $12.9 Million, plus another $1.4 million in bankruptcy fees, totaling $14.2 million. This estimate is exceptionally conservative as it is hard to put a monetary value on public sentiment and other side effects. Also, all 45 employees of DigiNotar had to find new employment to support themselves and their families in proceedings related to the bankruptcy.

As for the Dutch Government, it lost a source of tax revenue and had to assist with DigiNotar's business operations and navigate the bankruptcy court. The Dutch had to handle the public relations (PR) nightmare surrounding this. At the same time, the government needed to buy and issue new certificates for the websites DigiNotar previously issued. While it is hard to put a monetary value on these events, we can safely assume that these events caused numerous problems for the Dutch Government and required the government to spend considerable time, effort, and money on events and solutions relating to the attack on DigiNotar. Alongside the economic effects of the attack, a sociocultural side-effect emerged. Researchers reported that the attackers compromised over 300,000 Iranian Gmail accounts during the breach, which did not sit well with the Iranian population and cybersecurity experts worldwide. It shed light on the implications of compromising a certificate authority, which seemed highly unfeasible at

the time, allowing companies and governments to study, analyze, and learn from the mistakes made while improving security.

Methodology

To accomplish this, the attackers had to compromise DigiNotar, a root certificate authority based in the Netherlands that issued SSL certificates to websites. They realized it would be challenging to breach a company like Google, so it went after a weaker link: DigiNotar. Their entry method was complex, requiring the attackers to conduct years of planning and surveying the infrastructure. Although DigiNotar allegedly had a variety of physical security measures in place, like hosting critical servers behind locked doors with biometrics and personal identification number (PIN) codes required to enter, it is unknown how the attackers gained initial access. There is no clear indication that the physical security measures mentioned above actually were in place or if they even would have prevented an attack from happening [10]. Compromising a highly reputable company like DigiNotar, given the alleged security measures in place, imposes a challenging task that requires patience and planning. A nation-state usually carries out attacks with this level of sophistication and planning due to the immense resources needed for an attack of this scale.

After the attackers got into the system, they took advantage of DigiNotar's reputation and issued fake SSL certificates to whomever they pleased. With this came the attackers' ability to create a server between Gmail and DigiNotar, allowing them to view the "encrypted" data traveling from the user to the website they were attempting to visit. By doing this, the attackers helped create a mass surveillance system that allowed the Iranian

government to closely monitor its citizens' emails. The attackers issued over 300 fraudulent SSL certificates.

Now, how can we be sure that Iran was behind this? The motive is certainly there, but alongside the motive is an important fact. While the attackers connected to the DigiNotar servers, they would typically use a VPN to hide the origin of their location. Luckily for the Dutch Government and the cybersecurity community, the attackers forgot to use a VPN in one instance, allowing the authorities to reverse-engineer the attack. With this, authorities could map it out step by step, which led them to conclude that there was no doubt it was the Iranian government [10].

However, there is another explanation: Instead of the Iranian government being responsible for the attack, some suggest it may have been an Iranian citizen who identified himself as a (then) 21-year-old Iranian student with the online handle "COMODOHACKER." Ironically, Comodo got his name from breaching another certificate authority earlier that year, named Comodo. Shortly after the breach of DigiNotar, COMODOHACKER released a detailed post on Pastebin, which can be found in Appendix J.

Comodo gained access by acquiring the username and password (PRODUCTION\Administrator and Pr0d@dm1n) from DigiNotar, claiming his motive was the Dutch Government's involvement with the Srebrenica Genocide. While his story makes sense, this attack still requires a highly sophisticated understanding of breaching networks and the internal security measures of DigiNotar, which points to the workings of a nation-state. A report published by Fox-It (an independent cyber security firm that

analyzed the security measures put in place for DigiNotar after the attack) claimed that for DigiNotar to issue a CA, two separate employees had to grant access to the request [25]. It also had its computer networks on isolated servers that did not interact with each other. Finally, to issue the certificate, an employee had to insert a physical keycard into a computer strategically placed in a heavily guarded room, which Fox-It described below:

"This room could be entered only if authorized personnel used a biometric hand recognition device and entered the correct PIN code. This inner room was protected by an outer room connected by a set of doors that opened dependent on each other, creating a sluice. These sluice doors had to be separately opened with an electronic door card that was operated using a separate system from any other door. Another electronic door had to be opened with an electronic card if entering from a public area." [25]

The question arises: Who was really behind the attack? While DigiNotar could have lacked strong usernames/passwords and physical security measures, it did not wholly ignore security measures [26]. Some experts claim that due to the immense resources required to penetrate the robust systems of DigiNotar, it had to be the collective effort of a nation-state. On top of that, issuing a fraudulent SSL certificate for Google created a vast surveillance system that would have been perfect for a nation-state like Iran with a history of censorship and suppressing opposing views. Emerging from the shadows is a second story, where Comodo hacked DigiNotar as payback to the Dutch Government and eventually turned the keys to the kingdom over to the Iranian government, giving it the ability to issue fraudulent SSL certificates for Google to conduct mass surveillance on the citizens of Iran.

Prevention

Interestingly enough, many cyberattacks, like the DigiNotar attack, boil down to a couple of unfortunate mistakes. Simple security measures, like robust credentials, make the attacker's job more challenging by not being able to brute-force passwords (Appendix E contains different types of brute-force attacks with in-depth explanations). In DigiNotar's case, the failure was not requiring solid usernames and passwords. However, even when iron-clad usernames/passwords are present, there must also be strong network security to prevent attacks. Although conflicting reports arise about DigiNotar’s defense capabilities, having separate systems on separate networks, different clearance for different roles, and training the employees on cybersecurity are all steps that DigiNotar should have taken when preparing its defenses for an attack.

Shamoon (2012)

Overview

On August 15th, 2012, in Saudi Arabia, people were sleeping late and taking the day off. Rightfully so, as it was a religious holiday with a majority of its citizens staying home, enjoying their time off. Unbeknownst to them, a massive state-sponsored cyber-attack was deleting vast amounts of data from Aramco, a Saudi Arabian state-owned oil company. The New York Times (NYT) estimated that 30,000 corporate, personal computers (PCs) had been wiped clean within a day, only displaying the image of a burning American flag [26]. Three-fourths of Aramco's computers were deemed inoperable due to the attack, a devastating blow to Aramco. Luckily for Armaco, it had segregated the systems from its corporate side of operations from its production side. While 30,000 computers being destroyed and wiped out is a devastating blow to any company, the segregated systems helped mitigate the financial impact on Aramco.

After the attack began, Aramco had no choice but to take it back a couple of decades, moving its corporate infrastructure and systems to paper. Instead of email, it reverted to using interoffice paper mail. Most offices ended up without phone service since the phones' infrastructure used voice-over IP phones, which were inoperable because they required an internet connection. Within hours, typewriters and handwritten ledgers got brought out and used by the ~55,000 employees employed by Armaco to continue normal business operations and reduce the financial impact of them having no access to their online systems [26].

The Cutting Sword of Justice claimed credit; see Appendix K for its message on Pastebin. As one can see, based on the message above, this appears to be a malicious, targeted attack that was politically motivated, a common theme for nation-state attacks, especially like Iran.

Interestingly, the group that claimed credit for the attack fell off the face of the earth after 2012. While The Cutting Sword of Justice appears to be a legitimate hacking group, the idea emerges: was The Cutting Sword of Justice a persona curated by the government of Iran to throw off investigators and governments into finding out who was behind the attack? Fake personas, fraudulent stories, false flags, and destructive malware are all examples of nation-state attacks (i.e., Iran) that continue to differ from other, more traditional cyber threats.

History

Al-Sauds regime, otherwise known as the House of Saud, is the royal family of Saudi Arabia. Composed of the heirs of Muhammad bin Saud, who was the modern founder of Saudia Arabia, the House of Saud kept its royalty through their strict ruling with the King of Saudia Arabia, which makes whoever holds that position an absolute monarch. Experts estimate that there are over 15,000 members of the royal family, with a majority of its estimated 1.4 trillion dollar net worth in the hands of about 2,000 family members. To put it into perspective, this is about 16x the wealth of the British Royal Family [28]. Most of the wealth from the House of Saud is determined using the assets involved in Armaco, a Saudi state-owned oil company. To put its wealth into perspective, Aramco's revenue is the sixth highest globally, only slightly behind Walmart’s revenue [29].

With money comes power, and power can make people change for the better or worse. In the House of Saud's case, it was the latter. Reports claim that members of The House of Saud treat their servants awfully – not just in Saudia Arabia [30]. In 2002, Saudi Princess Buniah al Saud was arrested and thrown in the Orange County Jail. Allegedly, the princess pushed her servant, Ismiyati Soryono, down 16 stairs and struck her multiple times. Ismiyati fled Princess Buniah, calling the police, and since the Princess did not have diplomatic immunity (which she claimed to have), the police arrested her three days later [30].

Treating servants the way it does is not necessarily the most inhumane event in the world, but the House of Saud commits far worse atrocities. The Cutting Sword of Justice's text posted on Pastebin claims that the House of Saud was sponsoring other atrocities in neighboring countries such as Syria, Bahrain, Yemen, Lebanon, and Egypt. Syria, for example, had a nasty civil war that began in 2011, with the House of Saud sponsoring the opposing side of the Syrian war, and countries like Iran backed the current president, Bashar al-Assad. At the time of the Shamoon attack, over 50,000 Syrians had been killed in the war, creating over 500,000 refugees [31].

Impact

Restoring ~30,000 computers rendered useless with their master boot records (MBRs) wiped clean was no easy task. Due to flooding in Vietnam, a significant delay in the production of hard drives was present, with a steady backlog of orders for various amounts in the global market. The House of Saud knew this, and they flew representatives directly to the factories to negotiate the purchase of every hard drive

currently on the manufacturing line [26]. Aramco paid way over market value for these hard drives, skipping everyone in line that had already had existing orders for months. Kubecka, an independent consultant based out of the Netherlands hired to help mitigate their losses, claimed, "Everyone who bought a computer or hard drive from September 2012 to January 2013 had to pay a slightly higher price for their hard drive" [26]. In February 2011, the average price of a 2TB hard drive was $79.99. A year later, the average cost of a 2TB hard drive was $237.27, almost a 300% increase [32]. Assuming the House of Saud paid close to MSRP for these hard drives, the 50,000 hard drives would have cost them around $10,000,000, assuming each hard drive was $200.

The actual financial impact is hard to calculate because there is no way to know what other expenses it incurred due to this attack since Aramco did not publicly release its financial data at the time. After being hired, Kubecka claimed a massive army of IT people was present, saying, "I've never seen anything like that in my life" [26]. Assuming it hired 150 consultants like Kubeca for six months each, paying them 100,000 US dollars (USD) each, that is another $15,000,000 spent on helping repair its systems.

Although these are large numbers, the most significant financial loss was due to its systems getting wiped out and destroyed. Aramco had no way to review contracts, coordinate with truck drivers (and pay them), and no way to communicate effectively with other corporate partners. Shortly after the breach, there were massive delays in production as they had to fax extensive contracts one page at a time to be reviewed by hand. These events likely caused a halt (or extreme reduction) in revenue, as buyers looked to other companies to purchase oil, ones that had not had their operations halted

by a massive cyber-attack. Officially, Aramco never lost a drop of oil from the attack claiming its sales and production were unaffected by the attacks [33].

The total financial impact of this attack is around $100,000,000, but it is hard to pinpoint an exact number for this due to the vast amount of unknowns around the situation. How much revenue did it lose over this attack? How much oil ended up in the hands of its suppliers for free? What extra expenses did Armaco incur due to this attack? It took Armaco over five months to restore operations to normal [26].

Methodology

Experts claim that it is probable that an insider had access to Aramacos systems and intentionally inserted a USB drive containing the malware onto an Armaco system [26]. Another possible explanation is that spear phishing emails penetrated the system. However, this occurred almost simultaneously as the malware infected the system from the USB drive. (Appendix F has examples of phishing and spear phishing for a further explanation of the topic). Interestingly enough, the attacker was never identified or found [26].

Once the attackers gained access to the system, whether it was via spear phishing or a USB drive, they went to work, spreading the malware to other systems rapidly, escalating privileges, and increasing access to the systems. Once the attackers obtained the correct credentials, they started installing the Shamoon malware, a form of wiper malware (see Appendix G for an in-depth explanation of wiper malware). The malware was officially named W32.DistTrack consists of three main components [35]:

- **Dropper** - the main component and the source of the original infection, which installs a handful of other programs
- **Wiper** - this component destroyed the systems by overwriting the MBRs, partition tables, and most of the files with random data. Once overwritten, the computer is deemed worthless.
- **Reporter** - this component reported the information about the infection back to the attacker

Usually, anti-virus software detects malware spreading from system to system. Unfortunately for the defenders, the attackers disguised the malware as a legitimate driver (Appendix H explains the importance of drivers in a computer system), allowing the malware to be transferred from system to system without interference or pushback. With everything in place, the attack "began" by executing the wiper, clearing the master boot records on the system, thus rendering them inoperable.

It is hard to pinpoint blame on Iran in this case, but the common consensus is that it did orchestrate these attacks. This attack was also not the first time the Shamoon virus appeared in a malware attack. It resurfaced again in 2016 in more attacks in the Middle East, with anti-US images also embedded in the malware.

Prevention

A common theme of these nation-state attacks is that they all use relatively simple methods of gaining initial access to the target system. According to experts, there are two hypotheses about how they gained access. The first is that the attackers injected malware via a USB flash drive. Experts claim that someone on the inside intentionally brought the

USB stick into the facilities and inserted it into the system, knowing the outcome. Another theory, allegedly happening simultaneously with the USB theory, claims that initial access occurred via spear phishing emails.

While screening every employee and ensuring they are not foreign spies might be complex and costly, Aramco could have implemented other measures to prevent infection via a USB drive. For example, an average Aramco employee should not have been able to insert random USB drives into their systems. Robust security measures, absent from Aramco's systems, should have prohibited collecting/downloading data from random USB drives or removing USB ports from computers altogether when possible. Stuxnet, discussed later in this study, used a USB drive two years earlier than this event, so it is well-known that this form of cyber-attack not only existed but was successful and feasible in other attacks worldwide.

Aramco could have defended against these forms of entry if its employees had proper cybersecurity training. This training would entail examining various phishing techniques, detecting anomalies in phishing emails that could have prevented this attack from the start, and explaining the implications of inserting USB drives into company computers.

Sands Casino (2014)

Overview

Due to the rising tensions between Iran and the US, talk of diplomacy and foreign relations occurred among the citizens of both countries. Everyone had their own opinion, and the Sands Casino CEO, Sheldon Adelson (who happened to be the eighth richest man in the world at the time with a $38B net worth [36]), made some interesting comments about negotiating with Iran over their nuclear facilities and the increasing number of cyber-attacks [37]:

> *'What are we going to negotiate about? I would say "Listen, you see that desert out there, I want to show you something." … You pick up your cell phone and you call somewhere in Nebraska and you say, "OK let it go." And so there's an atomic weapon, goes over ballistic missiles, the middle of the desert, that doesn't hurt a soul. Maybe a couple of rattlesnakes, and scorpions, or whatever. Then you say, "See! The next one is in the middle of Tehran. So, we mean business. You want to be wiped out? Go ahead and take a tough position and continue with your nuclear development. You want to be peaceful? Just reverse it all, and we will guarantee you that you can have a nuclear power plant for electricity purposes, energy purposes."'*

Iranians were itching for revenge. As one might assume, Iran reacted swiftly and promptly to his harsh comments on its homeland. The Supreme Leader (Ayatollah Khomeini) released a statement shortly: "if Americans are telling the truth that they are serious about negotiation, they should slap these prating people in the mouth and crush

their mouths" [38]. Ironically, immediately after the comment, Iran's cyber force went to work, probing the network for any flaws it might find.

After entering and breaching the network, the attackers deployed a "malware bomb" that destroyed computers and stole troves of valuable data. Some affected networks included its loyalty rewards program, a million-dollar storage system, and the program that monitors the performance and payout of slot machines and table games at its US casinos. It is safe to say that this attack drastically affected its daily operations, resulting in a temporary loss of revenue and an embarrassing PR moment for the company.

This attack was unusual because the attackers demanded no ransom for the stolen data. Instead, where a ransom note would have appeared, there was a different message: "Encouraging the use of Weapons of Mass Destruction, UNDER ANY CONDITION, is a Crime" [37]. Some other experts say the attack traces back to Iran, although Iranian "hacktivists" most likely carried out the attack rather than the government. While this could be true, Iran is notorious for using contractors in its cyber army, hiring them for short periods or a specific job. This could explain why the attack was traced back to hacktivists, not the government.

History

Ironically, the US helped bankroll Iran's nuclear program (which originated as a research facility for medical devices), with the first nuclear facility (Tehran Nuclear Research Center) constructed in 1967. Contrary to today, Iran and the US were close allies, with the Shah spending billions on the US defense industry. The Shah had envisioned that nuclear energy would accelerate Iran into becoming a dominant world power by pledging

to construct up to 23 nuclear power plants by 2000 [42]. Instead, the citizens of Iran had other plans.

After the fall of the Shah, Iran continued to accelerate its nuclear program. In 2002, an independent group of Iranians presented evidence that the government was building nuclear facilities near Natanz. Shortly after, the Atomic Energy Agency visited the site to inspect what it had made. To its surprise, the findings showed that Iran had a much more sophisticated nuclear facility than US intelligence agencies had assumed. Another nuclear agency, the International Atomic Energy Agency (IAEA), reported that Iran was "enriching" its uranium, a process used to develop nuclear weapons. After discussing with its internal board of governors, the IAEA decided it was in the world's best interest if Iran suspended its nuclear enrichment activities. Iran refused to do so, and the UN and US imposed sanctions. Eventually, Iran folded and stated that it would no longer use the enriched uranium for nuclear weapons, turning the already-enriched uranium into fuel rods. Additionally, Iran would be open to outside committees, such as the IAEA, to monitor its nuclear sites. While this deal highlights Iran's willingness to adapt to the western countries' demands, unfortunately, the US declined this deal, claiming that it did not meet the UN's demand to dismantle its nuclear enrichment program altogether [39].

Impact

After the attack, reporters discovered through interviews that the attackers had wiped upwards of three-fourths of the company computer servers in Las Vegas. A source familiar with the company stated that it would cost over $40M to repair and restore those servers [41]. While that is a large amount of money, the attacks had no little effect on the

daily operations of the casino. It was chaotic internally, and it even had to disconnect the company operations from the internet. However, even with those drastic measures, hotel guests could still swipe their keycards to enter their room, and gamblers could still place bets at the blackjack tables and drop coins into slot machines. Ultimately, the customers kept gambling without knowing what was happening behind closed doors. Fortunately, the Sands Casino experienced little to no revenue loss since casinos could continue letting customers gamble. However, its stock price did drop 50% in the following seven months of Adelson's comment, wiping $25 billion worth of valuation from the company [40].

Learning from the mistakes made by Sands Casino, companies can prepare themselves to reduce the chance of a Cyber Attack from various hacktivist groups and nation-states. Corporations all over America use this as an example of why they should have robust defense mechanisms paired with an experienced IT team. Most importantly, organizations learned the implications of talking like Adelson did about Iran and other nation-states.

Methodology

First, the attackers launched a brute-force attack targeting one of Sands Casinos VPN portals in Pennsylvania. Their first step was a strategic play - the Pennsylvania office was a weak link in a large, worldwide organization. The IT team at Sands Casino was alerted of the thousands of login attempts and hosted an emergency meeting. Despite the thousands of fraudulent login attempts, no alarm rang. Second, on Feb. 1, attackers breached a Microsoft IIS development and staging server for the casino's website and

used open-source software to capture the usernames and passwords of the users. This website tested any Sands Casino website before it got published - acting as a test environment for any future updates made to the website. Brute-force attacks occurred in almost 50% of the companies, so the IT team downplayed the importance of these events.

Once inside the Microsoft IIS server, they used a tool called Minikatz, which revealed the usernames and passwords of users as they logged onto the server. Eventually, they hit the jackpot and gained access to a senior systems engineer who visited the site from Las Vegas, allowing them access to the ‘master network.’

While combing through the master network, the attackers deployed a malware bomb that destroyed computers and stole troves of valuable, sensitive data. This malware consisted of only 150 lines of code [42], and the script instructed the computer to erase all complex drive data and restart the computer. While restarting, the malware replaced the MBR with a random combination of 0s and 1s, rendering the system useless.

On February 10, ten days after breaching the Microsoft IIS server and escalating privileges, emails stopped working, phones stopped ringing, and the hard drives were wiped clean. Users' systems displayed a blank screen after the malware removed the data from hard drives. IT was scrambling, unsure of what to do, and it noticed something catastrophic in its logs: the attackers had compressed large amounts of data into zip files to steal large datasets. These datasets consist of credit checks of high net-worth clients, detailed diagrams, and inventories of global computer systems. After being notified of the situation, the president told IT to pull the company off the internet and disconnect it completely, giving the defenders a step ahead.

Another intriguing record discovered on the logs by IT: Iran's first target was the company's active directory servers. These servers offer two main functions; the first is managed network security, which is likely why the attackers chose this target. The second was that it provided a trusted and secure pathway to its operations overseas in Singapore and China, which were considerably more significant targets than the US operations in Las Vegas. While the move was strategic for continuing their attack, Iran lost access to a much larger target that would have been more catastrophic to the Sands Casino organization.

The following day, on February 11, the attackers started to deface various Sands Casino websites. Multiple pictures of the American flag burning would appear on websites, along with embarrassing photos of Adelson, the Sands Casino owner. The attackers even posted a personal message to Adelson, “Damn A, Don’t let your tongue cut your throat.” Eventually, IT restored its systems and resumed normal operations [41].

Prevention

First, a report claims it only had five IT members servicing 25,000 about two years before the attack [41]. While the board had approved various upgrades to personnel and tools, it was still in its infancy when Adelson made his claims about his opinion on handling Iran and its nuclear program. If Sands Casino had been more prepared regarding its IT operations, it might have been able to secure some of the cracks in the security that the attackers exploited. The Sands Casino attack shows the importance of having a good IT team that is up-to-date with attackers' current techniques and the technology to help

mitigate these attacks. When companies underfund their IT department, as Sands Casino did, attackers can exploit that weakness to destroy and compromise a company's servers.

As mentioned in the impact section, another way to prevent attacks from nation-states is to avoid speaking harshly toward states like Iran and North Korea. When someone openly says that the US should nuke them as a sign of strength, all one is putting a massive target on one’s back. Adelson was one of the wealthiest people on the planet, and with money comes power. Adelson thought he was invincible, and the Iranian Government had to humble Adelson and remind him that he was not invincible.

Section 2: North Korea

The Beginning

In 1945, after WWII, Korea was occupied by two central powers: the US in the south, with the Soviet Union occupying the north. The Soviet Union let the northern Koreans create the Democratic People's Republic of Korea, with Kim ll-sung as their leader. He built the nation with an emphasis on *Juche,* or self-reliance. Eventually, Kim Jung-un took over after his father's passing (Kim Jong-il, the supreme leader after his father, Kim II-sung, the founder of the People's Republic of Korea) and offered better direction for the country's cyber skills. Kim Jong-un's early life had an essential role in the creation of one of the largest cyber armies in the world. He was the first supreme leader from North Korea - his father had been born in the Soviet Union, and his grandfather was born when Japan ruled Korea.

Kim Jong-il had secretly sent children kids to Switzerland for school, where Kim Jong-un attended the Liebefeld Steinhölzli state school in Köniz under the name "Pak-un" or "Un-pak." From the mid-1990s until 2000, Kim disguised himself as the son of an employee of the North Korean embassy in Bern, a nearby city. While tracking his movements and timelines is difficult, researchers have concluded that Kim Jong-un had been living in Switzerland as early as 1991 [43]. The Laboratory of Anatomic Anthropology at the University of Lyon, France, made an astonishing discovery: they compared a photo taken of "Pak-un" while studying at Lievefeld in 1999 to an image of Kim Jong-un in 2012, concluding that the faces presented in both pictures have a 95% similarity.

Friends of Pak-un credited him as being shy with girls, well-integrated into the school, indifferent to political beliefs, and an avid basketball fan. Kim would brag to his friends at school, showing them a picture where he appeared alongside Kobe Bryant and Toni Kukoč. While he genuinely loved basketball, this was not the same for his study habits; he allegedly did not perform well at Liebefeld. However, Kim did take computer science courses, potentially sparking his interest in cybercrime and the computer world.

Kim Jong-un would continue his education back in his home country, North Korea, attending Kim II-sung University, majoring in physics, and attending Kim II-sung Military University, graduating as an army officer. His education proved critical to his methodology of governing cyberwarfare and its beloved nuclear program. Back in their home country, where nights are pitch black and food is scarce, the people of North Korea have no contact with the outside world. Only 1% of the population has access to the internet, and only a few Americans have entered the country [44]. Over time, North Korea has committed hundreds of crimes as it ramped up its Cyber Army. One notable attack is The Dozer Attack which affected numerous financial institutions in the US and South Korea, effectively creating panic and fear in their target populations.

Dozer Attack (2009)

Overview

In July 2009, a sophisticated cyber-attack started to unfold; dozens of banking websites in both South Korea and the US went offline, with the attack infecting about 50,000 computers. While the attackers did not demand monetary compensation or a ransom, they were very effective at their tasks. By crippling the bank's online services, they could not process basic customer requests like withdrawing money and checking account balances. As the attackers expected, trust in these financial institutions fell drastically. Consumers started to panic without access to automated teller machines (ATMs), in-person branch withdrawals, and other essential bank functions. This resulted in the loss of the fundamental trust required to operate a business as necessary as a bank. If individuals cannot access their money instantly, they will not want to bank with that company, which is precisely the idea behind an attack like this. The attackers likely attempted to create a domino effect of people withdrawing money and not depositing, creating a run on the banks, which can devastate the company and the country's economy. However, South Korea has a strong economy, which makes it more probable that the attackers wanted to instill fear and uncertainty in the population instead of crippling the financial sector.

While the attackers initially did not seem to want any damages beyond a distributed denial-of-service (DDoS), when attackers send thousands of requests to servers to overload them, preventing legitimate requests from reaching their destination, this eventually proved to be false. The DDoS attacks started on July 4 and lasted until July 10,

when the next attack phase started. The following US and South Korean websites were affected [46]:

banking.nonghyup.com

ezbank.shinhan.com

ebank.keb.co.kr

www.nyse.com

finance.yahoo.com

www.usbank.com

www.ustreas.gov

Interestingly, the attackers' DDoS was initially relatively simple and easy to recognize and sort out the fake requests. However, as the days went on, the DDoS became more sophisticated, getting better at mimicking actual requests, making it harder for the defenders to select and remove the malicious requests. The attackers coded within the malware to terminate the DDoS attacks on the 10th and initiate the next phase, destruction. First, the malware began deleting specific file extensions (such as .doc, .pdf, .xls, and other business-type files [45]) as it carried out the malware. Then it started deleting the MBRs of the infected systems, rendering them useless and displayed the message “Memory of the Independence Day” - signaling that a larger group carried out this attack, most likely a nation-state, instead of a lone wolf [46].

History

North Korea and South Korea have always been rivals since their founding, embracing dramatically different political and cultural views. North Korea aligned itself with other communist and authoritarian regimes, most notably Russia and China, embracing self-reliance since its inception. South Korea sides with the western world and is one of the US's most significant allies.

North Korea is also ambitious in developing its nuclear weapons program and has received many sanctions over the years because of its involvement in nuclear warfare. At first, sanctions targeted the trading of natural resources, which was North Korea's main export. Then it led to sanctions on the import of high-class items like alcohol and Rolls-Royces to target the elitist group of North Korea. Sanctions were also placed on various financial institutions in North Korea, cutting off their access to the USD, which hindered Kim Jung-un's ability to acquire his luxury items, even off the black market. These sanctions led Kim to develop new methods to gain USD, most of which involved sophisticated, thought-out attacks by his personal Cyber Army.

Impact

The era of this attack, 2009, was the first instance of the widespread use of DDoS attacks to take down the financial industry and instill chaos in a population. The attacks, thought out and well-planned, took time to guarantee success. Government officials and corporations worldwide saw this, reacting swiftly by upgrading their defenses and learning how the attackers gained access, investing in cybersecurity training for their employees to help prevent an attack like Dozer from occurring again. Researchers also

studied how people responded to the temporary shutdown of the financial industry and how quickly chaos can occur, shedding light on the societal impact of an attack like this.

This event escalated tensions between South Korea and North Korea, and their allies followed suit, adding to the enormous divide we see between "east and west" countries, or authoritarian, traditional style governing and democratized, western countries. This divide fueled many wars, most notably The Cold War between the US and the Union of Soviet Socialist Republics (USSR) in the 1950s and 1960s. North Korea was fighting fire with fire, with no attempt to de-escalate its diplomatic situation despite pressure from its allies and the international community.

Methodology

Researchers and the public coined these attacks "The Dozer Attack" after the name of the infection files used to execute the attack. The attack began with phishing emails containing four files disguised as malware. The malware, highly advanced for its kind, infected systems at an astronomical rate with no detection while installing backdoors to the infected system. See below for Table 1 dissecting the four malware files that facilitated "The Dozer Attack."

W32.Dozer	**Helped facilitate the release of the other malware**
Trojan.Dozer	**Provided the DDoS and a backdoor**
W32.Mydoom.A@mm	**Deployed a worm, spreading the malware to additional systems**
W32.Mytob!gen	**Infected the victim's system, allowing access to their email, sending Trojan.Dozer to their entire contact list**

Table 1 - Malware Files that Facilitated "The Dozer Attack"

Once the attacker had amassed ~20,000 computers around the world acting as a botnet (a collection of compromised computers controlled by a third party), the attacks began. When initiated, the malware had exponential growth with the W32.Mytob!gen file forwarding the malware to the infected systems contact list. The attackers were also cautious about covering their tracks, using botnets purchased by other cybercriminals or other unregulated means, which hindered the investigators' ability to trace the attack to its origin.

With a relatively simple method of gaining access to one's system (phishing) paired with the execution of W32.Mytob!gen allowed for explosive growth with minimal effort required. The worm permitted the attackers to rapidly expand the infected pool of systems with minimal effort, all remotely, without any manual input from the attackers. Once they infected the first system, they created a “snowball effect” of people clicking on

the phishing link received from patient zero, infecting their contact list and spreading the malware to more victims. Using botnets obtained through untraditional means, the attackers masked their identity, and authorities could not trace the attack's origin.

Despite the botnet, several facts connect North Korea to The Dozer Attacks. First, the attack happened simultaneously as North Korea conducted un-sanctioned ballistic missile tests. Second, the message displayed on infected systems, “Memory of the Independence day,” was anti-American. While countries like Iran, China, and Russia center themselves around an anti-American ideology, South Korean and US banks' specific targets point to North Korea-facilitated attacks. In 2014, the US formally declared that North Korea was behind these attacks [46].

Prevention

A common theme across these case studies is that initial access is the hardest part of the attack while simultaneously being the easiest part. Spear phishing and flash drives are typically the primary means of entry with nation-state attacks. As for The Dozer Attack, spear phishing emails provided initial access to the attackers. After initial access, the malware rapidly spread to the infected contact list, creating exponential growth in the number of infected systems. Organizations realized the implications of clicking a single link that can allow attackers to advance quickly to the next attack stage, gaining access to more systems with higher privileges. Defenders mitigate phishing with proper employee training, explaining the implications of clicking on a phishing link or inserting a random USB drive into a work computer. Financial institutions worldwide must have strict cyber-security practices to prevent an attack like this from happening again and again.

Bank of Bangladesh (2016)

Overview

Since the introduction of sanctions, North Korea has been openly hacking multiple financial institutions worldwide, stealing hundreds of millions of dollars to support their nuclear program and their supreme leader's lavish lifestyle. The Bank of Bangladesh was the victim of one of the largest robberies ever committed by a nation-state to date, and it occurred in 2016 when these large-scale financial thefts were still relatively new. The robberies likely originated from vast sanctions and embargoes put on North Korea for its involvement in developing nuclear weapons, requiring North Korea to become self-sufficient since it could not trade with most of the world. Instead of backing down on its nuclear program as western leaders had hoped, it embraced becoming one of the world's most prominent supporters of organized crime. What is the response to the sanctions? Fight fire with fire.

The US Department of Justice has released reports on North Korea's previous hacks and has developed an 8-step process consistent with attacks stemming from NK, which include the following steps: [50]

Step 1: Reconnaissance

Step 2: Initial Compromise

Step 3: Observation and Learning

Step 4: Enumeration and Privilege Escalation

Step 5: Preparing the Stage

Step 6: Execution of Fraudulent Transactions

Step 7: Timing the Transaction Attempts

Step 8: Deleting Evidence and Covering Tracks

These eight steps are evident in the Bank of Bangladesh attack and many later attacks. The methodology section will discuss these steps concerning the Bank of Bangladesh attack and how a North Korean operative named Park could orchestrate an attack of this magnitude.

History

North Korea and the US have a history in diplomacy, with most of the tension arising from North Korea's nuclear program and its authoritarian style of ruling and anti-western views. On December 12, 2012, North Korea launched its first satellite into orbit, Kwangmyŏngsŏng-3 Unit 2. While one might not see the problem with this, the UN had imposed a ban on North Korea's ballistic missile tests, and the technology behind ballistic missiles and satellite launches are surprisingly similar. The satellite's main job was to survey Earth. The South Korean Government and NORAD confirmed that an object had achieved orbit, despite the Kwangmyŏngsŏng-1 and Kwangmyŏngsŏng-2 (earlier attempts at launching a satellite) failures and never reaching orbit [47].

After the launch, countries worldwide and UN officials were furious. The US condemned the act as an irresponsible decision that threatened regional security, and even China, one

of their closest allies, expressed regret over the situation [50]. In response, the UN passed United Nations Security Council Resolution 2087, urging North Korea to “not proceed with any further launches using ballistic missile technology” and to “re-establish its pre-existing commitments to a moratorium on missile launches” [48]. North Korea responded by officially rejecting the resolution, putting more strains on their diplomacy over their nuclear program.

Impact

Since the Bank of Bangladesh attack was one of the first of its kind - it shocked the world as the story quickly gained traction like wildfire, with various media organizations spreading the story promptly and rapidly. As the story made its way around the globe, so did fear. Before this, bank robberies usually consisted of a couple of criminals entering regional branches or other physical sites to obtain large amounts of cash or valuable items. Some of the largest robberies have been committed this way. Notably, the Belfast Bank heist in 2004, where attackers held an executive's family hostage and demanded access to high-security vaults, taking over $53M, and they were never found or caught. There is also the Banco Central Heist in 2005, where a group of criminals created a landscaping company as a cover to dig a 256-foot tunnel in the ground leading to a vault containing $71.6M of cold hard cash[49]. Although, until this attack, nobody had even envisioned a billion-dollar robbery to occur without gaining physical access to the bank. The bank's $101M in USD went missing from fraudulent transfers.

Unfortunately, police in Bangladesh arrested two employees of the bank that had the responsibility of initiating and approving money transfer instructions but were later freed

without being charged. Even with no charges, the arrest and appearance of guilt likely hindered their professional careers and embarrassed their family and friends. None of the criminals saw the inside of a jail cell, and authorities did not recover most of the stolen funds. After the attack, governments and corporations worldwide urged the Society for Worldwide Interbank Financial Telecommunication (SWIFT) to recognize that it was the big fish for cyber-attacks and that SWIFT needed to beef up security drastically, or else attacks like this would continue to happen [46].

Methodology

The attackers used the eight-step process in the Bank of Bangladesh attack in 2015, and we will break it down step-by-step below using the facts from the attack:

Reconnaissance: A year before the cyber-attack began, Park conducted online surveillance. He would gather information about the bank's strengths and weaknesses, attempting to find vulnerabilities in their network. Along with the bank's infrastructure, Park had researched the bank's website, employees, email addresses, and even the employees' social media accounts. During this time, the attackers created target lists of people and their associated email addresses to help understand their targets and create a method for compromising the systems initially. In some cases, the attackers made email addresses to curate a fake social media profile, later used to send spear phishing emails to vulnerable targets.

Initial Compromise: Spear phishing was the most used method in this phase to obtain initial access to the system, which is what the attackers did with the Bank of Bangladesh. Attackers used the information gained in the reconnaissance phase to tailor their phishing

emails to the target. U.S investigators have said that North Korean hackers create curated emails that are “highly targeted, reflect the known affiliations or interests of the intended victims, and are crafted--with the use of appropriate formatting, imagery, and nomenclature--to mimic legitimate emails that the recipient might expect to receive” [50]. The attackers knew their target's daily routine, what reports they were expecting, whom they were receiving them from, the specific communication vocabulary, and who their victims would frequently carbon copy (CC). The attackers spent considerable time and effort learning, targeting, and creating these spear phishing emails.

Once they compromised an account, they could leverage this to compromise more accounts by sending more spear phishing emails from legitimate email addresses to people with more authority in the company. Due to their reconnaissance, the attackers CC’d people they knew were supposed to be CC’d. While they were not the target, it helped create the illusion that these emails were legitimate.

Another method of gaining the initial compromise was by using public-facing email addresses. A public-facing email address is an email address that is not assigned to a specific person but rather to a team of individuals, usually in a business sense. It is available to the public, usually for submitting information and files related to the business. For example, at the Bank of Bangladesh, a team operated a public-facing email address used for people to submit resumes and other official correspondence. The attackers knew this and sent a resume with malware attached to it. Once opened, the infection began, allowing attackers access to the systems and networks of the company.

Observation and Learning: This part requires the most patience. After the initial compromise, the attackers must continue learning the target's environment and solidly understand their day-to-day operations. Based on previous attacks, North Korea is known for its patience and planning, often taking several months and even years to facilitate an attack on its victim. At the time, this was unheard of, especially in the financial sector. After all, this was the first “big” robbery attempt, and the Bank of Bangladesh lacked preparation.

Their observation of the Bank of Bangladesh eventually paid off. The attackers realized a key fact for the Bank of Bangladesh (and later the Tien Phong Bank in Vietnam): They archived their SWIFT transactions differently. The Bank of Bangladesh printed these transactions on paper and stored them as hard copies, while the Tien Phong Bank in Vietnam kept them in a portable document format (PDF) using Fox-It PDF software to read these documents. At the Tien Phong bank, they installed a weaponized version of Fox-It that infected employees' computers when they accessed these documents. Identifying each bank's unique practices created a highly customized attack targeting its weak spots. Since they knew that the Bank of Bangladesh printed hard copies of their SWIFT transactions, they knew that this method of attack proved unfeasible for the job in Bangladesh.

Enumeration and Privilege Escalation: Using various tools, most obtainable online, the attackers could enumerate and gain valuable information on the victim's networks. The goal ultimately was to figure out which computers sent and received SWIFT transactions and communications. However, SWIFT had some security measures already in place. It had a segregation of duties policy that separated privileges across multiple people, so not

one person had access to the entire SWIFT network. While, in theory, it seems practical, this was not the case for the Bank of Bangladesh. All the attackers needed to do was gain access to more systems, using tools like a keylogger to gain login information or using various spear phishing emails. With the Bank of Bangladesh, evidence shows that one of the victim's computers had a keylogger under C:/Windows/Web/Wallpaper/Windows. This likely means that the malware came as wallpaper, and the victim downloaded it and installed it on their system. To advance to the next stage, attackers must realize their specific targets and the privileges needed to gain access, which is what the attackers do in this stage.

Preparing the Stage: In this stage, attackers must keep their presence undetected, which poses challenges because they usually have external communication to communicate with the malware. In building the tool for maintaining control of the malware, the attackers created a “custom binary protocol designed to look like TLS Traffic” (transport layer security, a method of encrypting network communication). TLS enables communications to travel between networks with encrypted data instead of clear-text, unencrypted data. With the attackers' custom TLS encryption, they could insert their keys into the encrypted data, making them the only subject to decrypt the TLS data. They masked their communication by creating a backdoor into the TLS encryption, enabling them to encrypt/decrypt their data at their own will while looking legitimate from an outside perspective. The attackers also had an additional layer of complexity with storing the backdoor in the memory of the infected systems versus on hard drives and solid state drives (SSDs). Usually, defense mechanisms, such as anti-virus programs, can detect when malware is present on a hard drive, so being on just memory alone creates this

added layer of security for the attackers. This method does have its flaws: by being stored in memory, it is susceptible to network restarts or reboots, but the attackers coded the malware to detect when a restart/reboot would happen, then copied itself to the hard drive to reboot when the computer restarted. After the system reboot, the copy is deleted from the hard drive and continues to store itself in memory. While complex, if someone were to unplug the computer, the malware would be destroyed because it does not indicate that a restart is coming.

Execution of Fraudulent Transactions: Using information gained in previous stages, the attackers logged on to the SWIFT Alliance application (a messaging software to conduct financial transactions). SWIFT requires multiple levels of security for this application, like being isolated and segregated from other bank networks, enforced with routers and firewalls, which all help secure the network. Unfortunately, as described above, robust security measures were not in place during the Bank of Bangladesh heist. According to the U.S Congressional Research Service, "Bangladesh's network may have been particularly vulnerable, as it reportedly lacked a firewall to protect against outside intrusion."

The lack of defense mechanisms put in by the defender was detrimental to the Bank of Bangladesh by creating opportunities for the attackers to exploit. The attackers attempted to create fake operator accounts, which would have permitted them to authorize transactions from the SWIFT Alliance application, but ultimately they were unsuccessful. The attackers were unsuccessful multiple times in attempting to log in to the SWIFT Alliance application. The defenders would have caught these attempts and avoided the attack if the proper security measures had been in place, alerting the defenders of the

invalid login attempts. The attackers likely knew that the defenses would be lax in countries like Bangladesh and selected them as targets. After they gained access to the alliance messaging board, they started to execute transactions, 35 in total, with over $1B on the line. From an outsider's perspective, the transaction attempts seemed legitimate, authorized by the correct accounts and raised no red flags.

Timing of the Transaction Attempts: The highly sophisticated attackers timed the transactions to happen usually after 11 pm and before midnight during the local time when the banks were closed. Alongside that, the attacks occurred during the weekend, when they knew the bank staff would be limited and their chances of success were best. This methodology is surprisingly standard in financial attacks of this magnitude.

Deleting Evidence and Covering Tracks: After experts and industry leaders analyzed the attack, they found that the attackers had composed their malware to detect and delete files containing evidence left during the compromise after it had completed a financial transaction attempt. The malware included deleting information on the system logs that could have helped the defenders realize what was happening in real-time. This malware was present in many other attacks orchestrated by the same nation-state, most likely North Korea [50].

Prevention

The Bank of Bangladesh attack showed the world why cybersecurity is crucial in the financial industry. Due to the lack of defense measures, it highlighted the importance of having up-to-date mechanisms and following cybersecurity guidelines imposed by SWIFT. If it had implemented even a single recommendation of defenses by the SWIFT

organization, it would have likely prevented this attack. The financial industry and organizations worldwide realized this, and more institutions beefed up their cyber security because of this fact. The front-line defenders must be adequately trained on the current and most relevant attack strategies so that their organization does not become compromised. With better security comes better employees.

FASTCash (2016)

Overview

In May 2016, the Yakuza crime family members were presented with a new task to make money. Shimomura, a crime syndicate member, was instructed to meet at a bar in Nagoya. While he was part of the notorious Yamaguchi-Gumi, one of Japan's most prominent families of the Yakuza crime syndicate, he took pride in his appearance, wearing fancy suits and matching loafers. Nonetheless, he was an errand boy, spending time collecting debt and doing odd jobs.

Upon arriving at the bar in Nagoya, three other gangsters were present, whom he did not recognize or know. Like Shimomura, the other three came of Korean descent, and they all conversed in Korean for a while. Eventually, the boss arrived, and the real work began. Everyone took a white credit card - no chip, numbers, or name - just the magnetic strip. The boss articulated several points from a manual - the next day, the members received instructions to go to any 7-Eleven and pull 100,000 Yen (~670 USD in today's dollars, ~900 at the time of the attack) 19 times - no more than 20 - from these 7-Eleven ATMs. They were to conduct these withdrawals from 5 am to 8 am and, when prompted, select the Japanese language. Shimomura soon realized that this was an indication that the cards were foreign. Nonetheless, they each memorized a PIN, received further instructions to wait an hour between ATMs, and were allowed to keep 10% of the cash for their trouble.

On Sunday morning, Shimomura dressed casually, wearing jeans, a t-shirt, a baseball cap, and sunglasses. He approached a 7-Eleven, inserted his white card into the ATM,

selected Japanese, and withdrew 100,000 Yen. To his surprise, it worked. He repeated this 18 more times. Upon examining his receipt, he could distinguish a foreign name on the receipt but could not assume its nationality - besides the fact that it was not Japanese. After completing 38 withdrawals across two 7-Elevens, he walked home with his pocket stuffed with 3.8M Yen, or about 25,000 USD in today's terms. He stashed his share in a drawer at his apartment, later meeting his supervisor to return the rest of the money. The superior told Shimomura that he would keep 5% of the profits and pass the rest up the chain of command to the people who orchestrated this fiasco. Shimomura assumed that his boss enlisted the help from many other "volunteers" - and he was right.

The following day, authorities claimed that over the equivalent of 16 million in USD was taken from 1700 ATMs nationwide, using data stolen from South Africa's Standard Bank. Reporters claimed that 7-Eleven was the target because it accepts all foreign cards at its ATMs. Soon after the attack, most ATMs in Japan had their withdrawal limit adjusted to 50,000 yen to prevent the potential losses of an attack like this.

Japanese authorities stated that shortly after the attack, the ringleader of the 7-Eleven operation crossed from China into North Korea. Little did Shimomura know he had been collecting money to support the Korean People's Army on behalf of the Lazarus Group [51].

History

North Korea made drastic changes from being almost completely isolated from the outside world to one of the most developed and sophisticated cyberwarfare nations. How did they develop into the cyber-attacking conglomerate that we know today? Well –

North Korea took notes from the US. According to a report in 2019 written by Korean scholars at Korea University in Seoul, Kim Jong-Il commented about cyberwarfare after observing what was happening with the US and the Gulf Wars (notably, American planes jammed Iraqi radar systems preventing detection). Kim concluded that “modern war is decided by one's conduct of electronic warfare.” A Korean People's Army book also quoted Kim, “If the Internet is like a gun, cyberattacks are like atomic bombs [51].” When his son, Kim Jung-un, came into power, he continued to build the legacy of North Korea with the advancement of his cyber army.

While the west has had sanctions in place since the 1950s, they started to ramp up around 2006 in response to the development of North Korea's nuclear army. Kim said that his army could “penetrate any sanctions," and that is what he did. Since North Korea has been under heavy sanction since its founding, it has had minimal access to the US dollar – making it difficult for Kim to support his lavish lifestyle. Kim's lifestyle consisted of “a personal harem of thousands of women” called the “Pleasure Brigade,” private islands, a string of palaces, and luxury vehicles – all requiring USD to purchase and support. His lifestyle is so important to him that in 2021 he demanded that the US lift sanctions on luxury items like high-class alcohol and suits before even discussing denuclearization [52].

Experts estimate that Kim Jung-un's cyber arms have between 3,000 and 6,000 members, officially named *Unit 121,* which is a subset of its larger group, the Reconnaissance General Bureau (RGB). Kim’s cyber army is responsible for stealing around a billion dollars annually to fund its regime [51].

Impact

There are several implications for an attack of this magnitude. First, the noticeable immediate financial impact was that the equivalent of 16M USD was removed from the ~1700 ATMs across Japan. While some of this money was recovered or covered by insurance, the defenders still lost a lot. Alongside this, there were repercussions for 7-Eleven, who, following the attack, reduced the withdrawal limits from 100,000 Yen to 50,000 Yen to mitigate the damages if another attack occurred. Governments also took note of the tactics used for this attack and beefed up their security to prevent them from exploiting the same vulnerabilities elsewhere.

Shortly after the attack, the ringleader crossed into North Korea with most of the proceeds, but this did not discourage the Japanese authorities from tracking down and arresting over 260 subjects. While most of these subjects were members of organized crime, they still were members of society with families and children. Assuming half had families, 130 families were potentially ruined over this attack for approximately 3-4 thousand dollars per person.

Methodology

To grant permission to the 14,000 fraudulent ATM withdrawal requests, the attackers had to compromise South Africa’s Standard Bank. While it is unknown how they initially gained access, some experts claim it was via spear phishing. After gaining initial entry, the attackers installed the Trojan.Fastcash malware onto the bank's Switch server, which relays ISO 8583 messages for SWIFT. In layperson's terms, they compromised the server responsible for transmitting sensitive data concerning financial transactions from the

SWIFT system. By doing so, they approved fraudulent transactions that originated from Japan using stolen customer data from South Africa's Standard Bank. Since 7-Eleven accepted any foreign debit card, the attackers picked it as their primary target and to be the center of this attack for its market presence in Japan [53]. See Figure 2 [54] for a detailed diagram of their methodology.

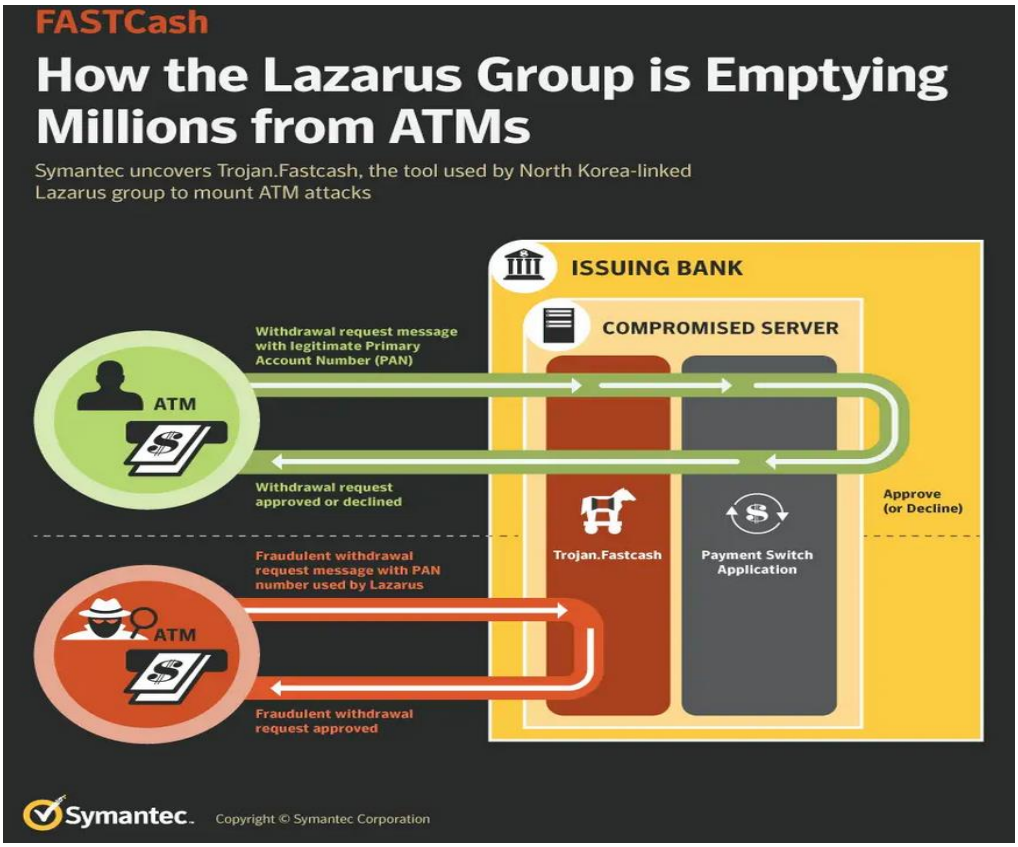

Figure 2 - How FASTCash works

Prevention

As mentioned in the “Impact” section, governments and corporations worldwide did not take this style of cyberattack lightly. Since an organized group attacked with a powerful crime syndicate, this set a precedent since most cyberattacks did not involve hundreds, if not thousands, of people who had to physically be at an ATM to carry out the attack,

whom all had unique roles to play. Usually, attacks were carried out by smaller groups or organizations, sometimes without ever stepping foot out of their home country. Organizations realized that with the advancement of technology and computers come advances in the types of crimes committed using technology, which is evolving at exponential rates, similar to cybercrime.

Because of the assumption that the initial compromise happened via spear phishing, although not proven, defenders could have easily avoided the compromise if the employees had received the proper training to detect phishing and spear phishing emails and realized the implications of clicking on a random link. North Korea's selection of the South Africa Standard Bank went along with its methodology of selecting targets in third-world countries, where their defenses are likely to be less robust and lacking standardization compared to US and South Korean banks. These banks are less likely to have a substantial budget for their cyber defenses, less training for employees guarding the bank, and are years behind in being up-to-date with their systems.

Section 3: Russia

Presidential Election (2016)

The Beginning

Since the fall of the USSR in December 1991, Russia felt cheated by losing its homelands in Ukraine, Estonia, Latvia, and all the other countries that gained independence from the USSR. While still holding most of its land, Russia and its president, Vladimir Putin, envied the old USSR and would make various attempts to reclaim the land they thought was rightfully Russia’s to claim. Most notable is Russia's 2014 annexation of Crimea regions in Ukraine and the attempt to continue reclaiming lands with the invasion of Ukraine in February of 2022. Western nations and NATO have come to Ukraine's aid, supplying them with high-tech military equipment and drones, giving Ukraine an upper hand against Russia. This instance is not the first time Russia has attempted to expand its powerful reach as a nation. Russia has a history of committing cyber attacks over the past ten years, deploying ransomware and malware into thousands of unsuspecting victims and even interfering with elections to promote candidates aligned with Russia's ideology and interests. Most notable include the 2014 Ukraine presidential election, the 2017 French presidential election, and the 2016 US presidential election between Donald Trump and Hillary Clinton.

Overview

John Podesta, the head of the Democratic National Committee (DNC), received a suspicious email from Google claiming that someone was attempting to log in to his

account. According to the email, an individual in Ukraine tried to log into Podesta's account, and Google requested that he changes his password immediately. Podesta, being wary, instantly sent the email to the head of information technology (IT) to ask for clarification. IT confirmed Podesta's suspicions claiming that his account was compromised, and urged him to change his password ASAP and turn on 2FA. 2FA, otherwise known as two-factor authentication, is an extra layer of protection where a user has to provide two forms of access to gain entry into their system, like entering a password and providing a code received from a text message. Unfortunately, IT left out a few key observations leading to his account being compromised by the attackers.

Following the initial breach, the attackers began surveying the environment and escalating privileges. A couple of weeks before the presidential election, the attackers released troves of data from the DNCs servers on a DC Leaks website. The data was easily sortable, having a search function to help sort through some 20,000 emails uploaded to the website weeks before the election. The attackers specifically organized DC Leaks to be accessible to the average American. This newly acquired information did not sit well with the Americans, likely impacting their vote for the 2016 presidential election between Donald Trump and Hilliary Clinton.

History

In 2014, Russia began its annexation of Crimea, with the military advancing into Ukraine and securing critical locations like airports and a communication tower. Simultaneously, Ukraine had been the victim of a massive cyber-attack that hindered its ability to keep its government websites running, along with its news stations and social media accounts. On

top of all that, Russia used a DDoS to target the phones of various high-level government officials and members of the Ukraine Parliament. With the military advancing, phones offline, and governmental officials unable to communicate with one another, the citizens of Ukraine started to panic [55].

These events escalated tensions between Russia and the US. Western officials from all around the world condemn this attack, including then-president Barack Obama. On March 14, he released new sanctions on Russia over their involvement in Ukraine and the Crimea annexation, claiming that “the referendum in Crimea was a clear violation of Ukrainian constitutions and international law, and it will not be recognized by the international community” [56]. Russia was not pleased with the US response. From its point of view, it was taking back its homeland since Ukraine used to be a part of the conglomerate known as the USSR.

During his run for the presidency in 2016, Donald Trump did not criticize Putin's involvement in Ukraine or criticize the Russian government at all. Trump has long-standing ties with the USSR and Russia. He attempted to build a Trump Hotel in Moscow, but while ultimately a failure, it shows his strong relationship with oligarchs in Russia, as they had to bail him out of his financial troubles. It is reported by the New York Times that Trump and 18 of his associates had direct contact with at least 140 individuals within Russia, including contacts in WikiLeaks (a national organization that publishes stolen documents from hacks around the world, including the documents leaked on dcleaks.com), all during his run for the presidency [57]. Trump was ultimately Russia's prime candidate for Presidency due to his lax stance on sanctions regarding Russia. Journalists believed that Trump owes Russian oligarchs various favors from their

previous business ventures. Russia would do everything in its power to take Trump to victory.

Impact

The compromise of the DNC is the most politically motivated attack of this study. Russia aimed to influence elections by leaking sensitive data from the DNC's servers. This data consisted of internal emails of various tactics regarding the DNC pushing Hillary to win the primary over Bernie Sanders, tactics for competing against Donald Trump, donor lists, and other information that did not reflect highly of the Democrats. Please refer to Appendix L for a detailed donor list that the attackers leaked and posted to DC Leaks. A majority of America had access to the stolen data, with news stations reporting the events as they unfolded. If anyone was on the fence about whom to vote for, the leaked emails and documents likely pushed enough people to vote for Donald Trump. Although Hillary won the popular vote by a small margin, Trump won the electoral college, cementing his victory as the 45th president of the US of America.

Overall, Russia showed the world what it could do with elections. They had previously been successful in disrupting elections in Ukraine in 2014 and will continue to be successful in the 2017 French Presidential election. Russia embraces a uniqueness in cyberwarfare, with a significant focus on its political agenda and doing whatever possible to accelerate its narrative. Our country might never be the same due to this event. In recent years, the political divide has grown as each side has become more hostile toward the other. Riots, insurrectionists breaking into the capitol, and increased tensions all helped create this divide between right and left. Each side is more and more hostile

towards the “enemy” side. Creating a massive political divide that only hurts our country was likely Russia's goal with their disruption in the 2016 Presidental Election.

Methodology

Below is an email that Podesta received on March 19, 2016 [58]:

```
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> john.podesta@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

Figure 3 - Podesta's Email from Google

Podesta made the intelligent decision by sending the email to IT for confirmation if it was a legitimate email. IT’s response [58]:

From: Charles Delavan <cdelavan@hillaryclinton.com>
Date: March 19, 2016 at 9:54:05 AM EDT
To: Sara Latham <slatham@hillaryclinton.com>, Shane Hable <
shable@hillaryclinton.com>
Subject: *Re: Someone has your password*

Sara,

This is a legitimate email. John needs to change his password immediately,
and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both.
It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at 410.562.9762

Figure 4 - IT's Response

IT had confirmed that Podesta's email was legitimate. Unfortunately for Podesta, IT failed to point out two critical parts of the email he received. First, the links to reset the password were not the same. Google provided a bitly link (a URL Compressor that shortens URLs to make them more user-friendly and easier to enter), while IT provided Google's official security link. IT did not comment on this or indicate that the original email was fraudulent.

Second, the email address appeared to come from *no-reply@accounts.googlemail.com*, but in reality, this was a trick known as spoofing, a tactic that displays a fraudulent address instead of its legitimate one. IT made no indication that the email address was spoofed or that it arose from an illegitimate source. Following IT's guidance, Podesta reset his password promptly upon receiving their email. Unfortunately for him, he clicked on the first link, the bitly link, which compromised his system, granting access to the

attackers. While his password still ended up being changed, he made a crucial mistake in his method.

Following the initial breach, the FBI alerted the DNC that their servers were compromised (which shows our intelligence agencies' skills and vast reach on society). It responded by hiring an outside firm, CrowdStrike, to help investigate. After this, a series of unfortunate events started to unfold. Several months before the US came out and publicly stated that Russia was behind these attacks, CrowdStrike jumped the gun and blamed Russia.

A couple of days after CrowdStrike publicly attributed the attack to Russia, DCleaks.com had been set up and released on the open internet, which was no coincidence. A day after DC leaks were released, a hacker by the online persona of Guccifer 2.0 arose and claimed credit for the attack. He posted a WordPress post claiming credit and posting various highly sensitive information regarding donor amounts and information [61]. Shortly after Guccifer made the website, he released another message [61]:

> “Worldwide known cybersecurity company Crowdstrike announced that the [DNC] servers had been hacked by “sophisticated” hacker groups. I'm very pleased that the company appreciated my skills so highly))) But in fact, it was easy, very easy. Guccifer may have been the first one that penetrated Hilliary Clintons and other Democrats mail servers. But he certainly wasn’t the last. No wonder any other hacker could easily get access to the DNC servers. Shame on Crowdstrike: Do you think I’ve been in the DNC’s networks for almost a year and saved only 2 documents? Do you really believe it?”

Guccifer claimed to be an independent hacker located in Romania with no ties to Russia. The creation of his WordPress site and posting of leaked documents directly conflicted with what CrowdStrike had assumed, that Russia was behind these attacks. The contradictory information poses an even more pressing question: who orchestrated these attacks?

Two theories emerged. First, Guccifer 2.0 was involved with various Russian agencies and intelligence. This theory ultimately was the CrowdStrikes theory. The second theory was that Guccifer was a Romanian hacker trying to interrupt the election and democratic process. As time passed, more details emerged, blurring the absolute truth even more. Researchers analyzed the metadata (data that provides information about other data). They confirmed that the files originated from the DNC's servers, meaning Guccifer did not acquire them another way, solidifying their claim that they were behind the attacks.

However, Guccifer made critical mistakes following his WordPress post. It is known that spear phishing emails compromised John Podesta's account, but Guccifer did not indicate this on his website. Instead, when interviewing with Motherboard (a reputable online publisher), Guccifer stated that “I hacked the server through the NGP VAN [software] [60].” The software he claimed to hack helped assist other political parties and fundraisers all over the country. Guccifer also provided detailed information on the infrastructure of the DNC to Forbes to help solidify its claim. While this seems plausible, CrowdStrike (and authorities and other investigators) found no evidence of the attackers on the NGP VAN software. While this seems odd, Guccifer had posted stolen documents to back up his claim creating confusion for the investigators.

Another mistake Guccifer made that was detrimental to his credibility arose from the Motherboard interview. During the interview, Guccifer reinforced his claim that Russia had nothing to do with the attack and that he was the independent party. Motherboard tested his claim, asking him a question in Romanian, his native language. He began to hesitate, taking much longer to respond than usual. Motherboard sent him another message, asking him if he would like to use Google Translate to help speed up his response. Although Guccifere eventually responded in Romanian, linguistic experts claimed that it was broken Romanian and that the message contained a variety of linguistic inconsistencies [60]. Guccifer grew frustrated and finally stopped responding to questions by Motherboard, effectively ending the conversation and creating a massive blow to Guccifers credibility. Ironically, if Guccifer had opted for an interview over email versus one live, he could have carefully crafted a legitimate response in Romanian.

Another mistake that Guccifer 2.0 made was that his online persona arose only days after CrowdStrike publicly attributed the attack to Russia. This likely meant that Guccifer's persona was created due to CrowdStrike's attribution to Russia to help deflect that claim. Creating a fake persona, such as Guccifer 2.0, requires ample time, planning, and coordination. Since Guccifer 2.0 arose hours before its first online post, was the account created spontaneously without planning or coordination as a reaction to CrowdStrikes' attribution of the attacks to the Russian government?

The third mistake Guccifer made is related to a time-stamp for the documents he released online to back his credibility that he was behind the attack. The “save” timestamp read “2016-06-15:05:42,” which happened to be hours before Guccifer had posted the stolen data online. The timestamp showed that the alteration of the stolen documents took place after the initial theft. Additionally, it showed a last-modified by in Cyrillic characters that directly translated to the name of a previous director of the Russian State Political Directorate, Russia's first secret police.

Figure 5 – Timestamp from a Stolen Document

The final mistake made by Guccifer 2.0 proved to be the most detrimental to his credibility. Usually, when Guccifer was online, he used a VPN to help mask his true

identity and location. On one occasion, though, Guccifer failed to activate his VPN before going online, revealing the actual location of the attacker: Moscow. After the presidential election, Guccifer 2.0 never appeared again, disappearing from the online world. Both the websites and social media accounts stay dormant to this day [60].

Prevention

Since this attack started with a spear phishing email, a relatively easy method of infection, this could have all been easily avoided with proper cybersecurity training and having a competent IT team. The DNC had neither of these in place. If IT had been more thoughtful and adequately trained, the initial infection probably would have never happened and would have either delayed or destroyed the attacker's plans. Although Podesta could have had better knowledge about phishing emails and spoofing, he did his part by sending the email to IT to review. IT failed to recognize the bitly link and the spoofed email address, which was ultimately the DNC's downfall.

Proper cybersecurity training is essential today because all it takes is one click on a link, and the system is compromised. With formal training, people can recognize the various simple methods of gaining access to a system to help prevent an attack from happening to them or their organization.

Section 4: United States

Stuxnet (2010)

The Beginning

The US has quite a history of being the “world's police force” by interfering with unstable countries whether or not its citizens agree with an intervention. Typically, the US takes a traditional path of intervention by putting boots on the ground, displaying the powerful force of the US military. In the past 100 years, the US involved itself in a majority of wars all around the world. Some examples include a military intervention in Lebanon (1982-1984), military intervention in the Somali Civil War (1992-1995), the Bosnian and Croatian War (1992-1995), Afghanistan (2001-2021), Yemen (2002-present), Iraq (2003-2011), and Syria (2014-present). The list goes on, but the point is clear: the US likes to get its hands dirty. Recently, the US has introduced a new method of war: cyberwarfare. Instead of putting boots on the ground, the US can cripple a country's infrastructure without ever setting foot in its homeland. The Stuxnet virus is the first modern instance of its use of cyberwarfare to do so. By crippling Iran's nuclear facilities, we set them back for years, hindering one of our most significant threats to democracy.

Overview

A nuclear facility in Natanz, Iran started to experience something unexpected: nuclear reactors began to rattle and shake, with the centrifuges operating at speeds far exceeding the safety standards set in place by Iran. The high speeds of the centrifuges damaged the

systems and equipment Iran uses to enrich their uranium. Spinning the uranium at high rates is a process uranium must go through to create nuclear weapons and other nuclear products.

For obvious reasons, the Natanz Fuel Enrichment Plant's location is mostly underground. Over 7,000 centrifuges are operating to extract U-235, an isotope of uranium used to build and construct nuclear bombs. The centrifuges spin at extraordinary speeds to separate the isotopes and then introduce a gas that eventually turns the isotopes into a physical, solid-state form that can turn into a nuclear weapon [62].

Unbeknown to the employees in Natanz, a massive cyberattack was on the horizon. The attackers, surprisingly, knew all the inner workings of the nuclear facility. When creating Stuxnet, the malware sped up centrifuge speeds, causing them to break violently due to high speeds, setting back Iran's nuclear program for a decade. Further research shows that four zero-day exploits were used in this attack (exploits that have never been used by attackers before), meaning this attack was highly sophisticated and thought out, taking vast amounts of time to ensure success. These facts point the finger toward a nation-state being responsible for Stuxnet.

History

The Stuxnet attack drastically affected Iran's nuclear program. During the Shah's reign, with help from western countries such as the US, he created the Atomic Energy Organization of Iran under the condition that Iran did not develop any nuclear weapons. After the fall of the Shah and the American embassy in 1979, Iran chose a new supreme leader, and he decided to start developing nuclear weapons despite warnings from

western world leaders. The US did not take its claim lightly and ultimately ended up retaliating against the development of its nuclear facilities. Doing so would require years of planning and surveillance to understand the facility and its correspondence.

Impact

Starting in 2011, Stuxnet was the most sophisticated cyber-attack known to humanity. With four zero-day exploits, cybersecurity experts combed through the code, learning anything they could. This attack took years of planning, leaving no room for error. Since this attack was politically motivated and not financially, it was a wake-up call to nations worldwide that anything is susceptible to cyberwarfare. Governments and corporations acted swiftly after this attack, beefing up security at their top-secret facilities worldwide using the knowledge gained by following the path of Stuxnet, accelerating the introduction of cyberwarfare into our daily lives. Alongside this, Iran's nuclear program was set back a decade, proving to be a crippling blow to one of our biggest enemies in the middle east.

Methodology

According to various media reports, the Stuxnet malware was placed on a USB drive and dispersed to five companies in Iran that the attackers believed would bring them to the Nuclear Enrichment Facility (NEF) in Natanz due to their involvement with the NEF. The attackers believe that one of these companies would eventually lead them to compromise the systems at NEF. The attackers displayed a vast amount of intelligence by attacking this way, they knew what organizations worked with Natanz, and they knew that their third-party organizations would likely have less cybersecurity than those at

Natanz. The intelligence the attackers had was another clue that it was the actions of a nation-state, as any individual finds it hard to come by this level of information about top-secret governmental locations.

Although never proven, it is likely that an employee at one of these five affiliate companies picked up the USB stick off the ground, walked past security measures in place carrying the USB drive, and eventually inserted it into a company computer. Some experts claim that this person had affiliations with Israels Mossad and was paid to complete the task, acting as a double agent for the US/Israel and Iran [64]. A month later, Gholam Reza Jalali, an essential Iranian military figure, publicly blamed Stuxnet on cooperation from the US and Israel [65].

Upon the USB's insertion, the infection began and spread rapidly, eventually gaining access to the NEF with a vast expansion rate using a worm. Once accessed, the malware programmed the centrifuges to speed at uncontrollable rates, destroying thousands of centrifuges currently enriching uranium.

Unusual at the time, the Stuxnet worm did not act traditionally, with the worm requiring no internet connection to spread from system to system. Instead, the creators built it to target systems not connected to the internet, spreading via local area networks. For example, one of Stuxnet's zero-day vulnerabilities targeted Windows systems that shared the same printer. Another exploited vulnerabilities in a Windows keyboard file and task schedule file to escalate the attacker's privileges on a machine and give them complete control of the system. The attackers had one goal in mind: they wanted this worm to

spread quickly and rapidly. By doing so, they had to construct Stuxnet like no other worm because the systems in Natanz were not connected to the internet.

Another interesting fact that shows the high level of sophistication and planning behind this attack was that researchers uncovered the Stuxnet payload in a public malware repository, which many anti-virus programs scan to check for malware. The malware had version number .500, compiled in 2005 [63]. The attackers were likely testing the anti-virus software to determine if it would detect Stuxnet. Also, an anonymous entity registered a domain that would later operate as the command and control center for the Stuxnet operations, registering the domain the same month as version .500 was compiled [63].

Prevention

Stuxnet was a small pawn in a giant chess game of multiple nation-states, their adventures, foreign policies, and intervention in world affairs. A few simple answers arise regarding preventing attacks like this in the future from the story of Stuxnet. First, promote peace, not war. Stuxnet was an attack vector by the US and Israel to cripple Iran's nuclear enrichment program. This very controversial program sat uneasily with western leaders such as the US, and Stuxnet was their retaliation. If the leaders of Iran and the US could put aside their weapons for once and work out their problems diplomatically, there would be no need to use a program like Stuxnet. Proper cyber security could have also prevented this attack, although unlikely due to the event's timing. Since Stuxnet occurred in 2011, when cyberwarfare was still in its infancy, cybersecurity did not get as much focus as it should have. Today, militaries, governments, and

corporations all over the world train their employees and personnel on the dangers of inserting such USB drives into systems, with some entities removing the ability to insert USB drives into their systems altogether. If Iran's nuclear program had a basic level of cybersecurity training for all employees, this could have prevented the attack from happening or helped mitigate the losses incurred.

Conclusion

An overall trend that emerges throughout the examination of these case studies is that people offer initial access almost every time. Attackers use three primary entry forms when targeting people: spear phishing, a USB drive, or an undercover operative. While it is much more complicated to prevent covert operatives than spear phishing emails and infection with USB drives, essential cybersecurity can still tackle 2/3 of nation-states' most common forms of entry.

With the DigiNotar/Gmail attack, the alleged attacker, Comodo, gained access by acquiring the simple username and password of an administrator account with elevated privileges. With the username of PRODUCTION\Administrator and password Pr0d@dm1n, Comodo gained access to DigiNotar's systems. The attacker used a man-in-the-middle attack to issue over 300 false SSL certificates, allowing entities like the Iranian government to see unencrypted data from Gmail servers and every email sent from over 300,000 Iranian accounts. This event shocked the world as its unusual for a reputable company like DigiNotar to be compromised. When investigators traced the IP address back to Tehran, confirming that the attack originated from the capital of Iran, this set a precedent for the ability of nation-states to orchestrate these highly sophisticated attacks. With conflicting reports on how the attackers achieved initial access and what security measures DigiNotar had in place, it is hard to pinpoint what went wrong. Although, if DigiNotar had basic levels of security in place (like segregation of systems, robust usernames/passwords, and cybersecurity training), the attacker's forms of initial access might have failed.

For The Dozer attack, attackers gained entry with a single spear phishing email. This email spread four malicious files with W32.Mytob!gen accessing the infected contact list, sending additional phishing emails to their entire contact list, accelerating the infected systems exponentially. With the chaos created by the focus on the financial sector, organizations worldwide took note of the attackers' methods. Realizing the origin of these attacks came from a single phishing email, defenders can implement basic cybersecurity training across the organization to help mitigate an attack similar to The Dozer Attack in the future. Employees who realize the implications of clicking on malicious links can become more careful when using company computers to mitigate similar future attacks.

The Sands Casino attack in 2014 differs from most of the case studies presented in this report. The attackers used brute force to crack the VPN's username and password, providing them access to virtual servers where they implemented key-logging software to gain access to a senior engineer's credentials in Las Vegas, where the real damage occurred. Organizations can learn many lessons from this attack, starting with allocating proper money to IT's budget. With a decent IT team, employees can be well-versed in the systems they operate, adequately staffed, and devote more time and effort to researching various tactics attackers use to gain access, relaying their findings to the employees. Organizations can also learn from the implications of a comment like the one made by Adelson to realize the impact of talking harshly to a nation-state like Iran or North Korea.

The Bank of Bangladesh attack proved one of the most complicated and sophisticated attacks out of these eight case studies. With the initial compromise happening via spear-

phishing, the attackers quickly elevated their privileges, allowing them more access to more systems. Using the eight-step process put forth by the US government, the attackers stole upwards of $100M from The Bank of Bangladesh. Since they were operating on outdated document storage methods related to the archive of SWIFT transactions, the attackers exploited this vulnerability specific to The Bank of Bangladesh. This attack highlighted the importance of organizations (specifically in the financial sector) in underdeveloped countries having proper cybersecurity methods since attackers knew that these organizations would have more lax cybersecurity practices.

The FASTCash attackers allegedly achieved initial access with a spear phishing email. Targeting a financial institution in an underdeveloped country allowed the attackers to exploit vulnerabilities that other financial institutions did not have. The financial industry saw this attack unfold and beefed up its internal defenses, updating systems and training its employees on how to spot a phishing email and the implications of clicking on random links and inserting random USB drives into a working company system. This selection method was a wake-up call for banks worldwide, especially in underdeveloped countries, as they realized that an attack could happen to them too.

On the other hand, Shamoon's initial access was achieved either by a compromised party inserting a USB drive into a company PC or a spear-phishing email. Although Aramco had ~55,000 employees at the time, strict hiring practices and background checks should be in place for every employee. Alongside this, Aramco employees needed cybersecurity training to ensure they knew the potential outcome of clicking on a link from a corporate

PC. Organizations worldwide learned from Shamoon how ~30,000 PCs were wiped all due to a singular phishing email that could have been averted with proper training and vetting of their employees.

Russia's compromise of the DNC's servers also vastly differed from the other cases in this study. While many of the cases were politically motivated, Russia's target of the DNC's servers proved unprecedented since there was zero monetary gain from this attack. The DNC's primary function as an organization was to advance its political agenda, not to make a profit. Organizations, specifically governments, need to note this type of attack from Russia, as attacks like these can happen to any country or governmental organization worldwide, disrupting their democratic process and increasing the political divide that the world sees today.

Stuxnet's infection was the US's first instance of cyberwarfare in the modern age. Composing of double agents and vast intelligence knowledge, the US government put considerable time and effort into planning and executing this attack. Although ultimately, the attackers were never caught, the public consensus is that it was a joint operation with the US and Israel to strike against Iran's nuclear enrichment facilities in retaliation for their continued development of nuclear weapons. The enemies of the US and Israel saw this attack unfold and knew that it could happen to them at any time. This set a precedent regarding cyberwarfare since the malware was used as a weapon to cripple another country's nuclear operations. Typically, countries conduct cyberwarfare to instill fear and chaos, meddle with elections, or steal money from financial institutions. Stuxnet's attack

did not fall into any of those categories, shedding light on the use of cyberwarfare on the battlefield.

Teaching employees and personnel the proper usage of their systems allow them to be fluid in the technical workings of their business activities. Alongside teaching proper use, organizations must show people the worst-case scenario that is described above in these eight case studies. People must know the implications of inserting a random USB drive into a work computer or clicking on a link that they think is legitimate but turns out not to be. They could inadvertently cause their systems to shut down, potentially losing billions of dollars. With the information presented in this research, organizations should take note regarding their cybersecurity, act accordingly to prevent attacks from happening to their organization and understand that most of these attacks start with a human error.

Since no two attacks were identical, there is no handbook or flowchart to follow when preparing one's defenses. Every case study comes with a new reason for the attack, exploiting vulnerabilities in a new and unheard of ways, but each attack is aimed to create chaos and damage to the target. Threats exist everywhere, in all industries, big or small. An organization might have seamless defenses, but that does not guarantee the avoidance of a cyber attack since cyberwarfare is evolving daily, encompassing new methods and tactics to attack unsuspecting entities.

Appendix A - The Islamic Revolutionary Guard Corps

The Islamic Revolutionary Guard Corps (IRGC) is a branch of the Iranian Armed Forces, initially founded by Ayatollah Khomeini after the fall of the Shah and the 1979 Iranian Revolution. While the Iranian Army (separate from the IRGC) defends its borders, the IRGC intends to protect the country's Islamic Republic Political System [11]. In other words, their goal was to prevent foreign interference and coups (ex. The 1953 Iranian Coup) and protect Iran's national security. It has been a designated terrorist group since it allegedly backed terrorist organizations such as Hizballah, Hamas, PIJ (Palestinian Islamic Jihad), and the Taliban, both financially and defensively. On April 24th, 2022, President Biden confirmed to the Israeli Prime Minister that they would keep the IRGC on the Foreign Terrorist Organization List [12]. It is still a designated terrorist organization today, with Saudia Arabia, Bahrain, and the US supporting this declaration.

Appendix B - SSL Certificates

Secure socket layer certificates, known as SSL, act as an extra layer of security by encrypting the connection between the server and the browser. Organizations and companies around the world use this to securely transmit data such as transaction information, personal details, and much more. Without this, information shared between the server and browser is unencrypted and open to prying eyes [13]. See Figure 6 for an informative explanation of how SSL certificates work.

Figure 6 - How SSL Certificates Work

Appendix C - VPN

VPN, or virtual private network, allows one to encrypt their data online and hide their identity. Various uses arise from a VPN; besides encryption, people can use VPNs to disguise their whereabouts and gain access to restricted, regional content (people can mask their location to appear in a different country to gain access to new media and entertainment). Usually, people (and attackers) use VPNs to hide their IP address, so they can freely receive and send information without fear of anyone knowing what they search and what websites they visit (besides their VPN provider) [14]. See Figure 7 for a better understanding of how VPNs work.

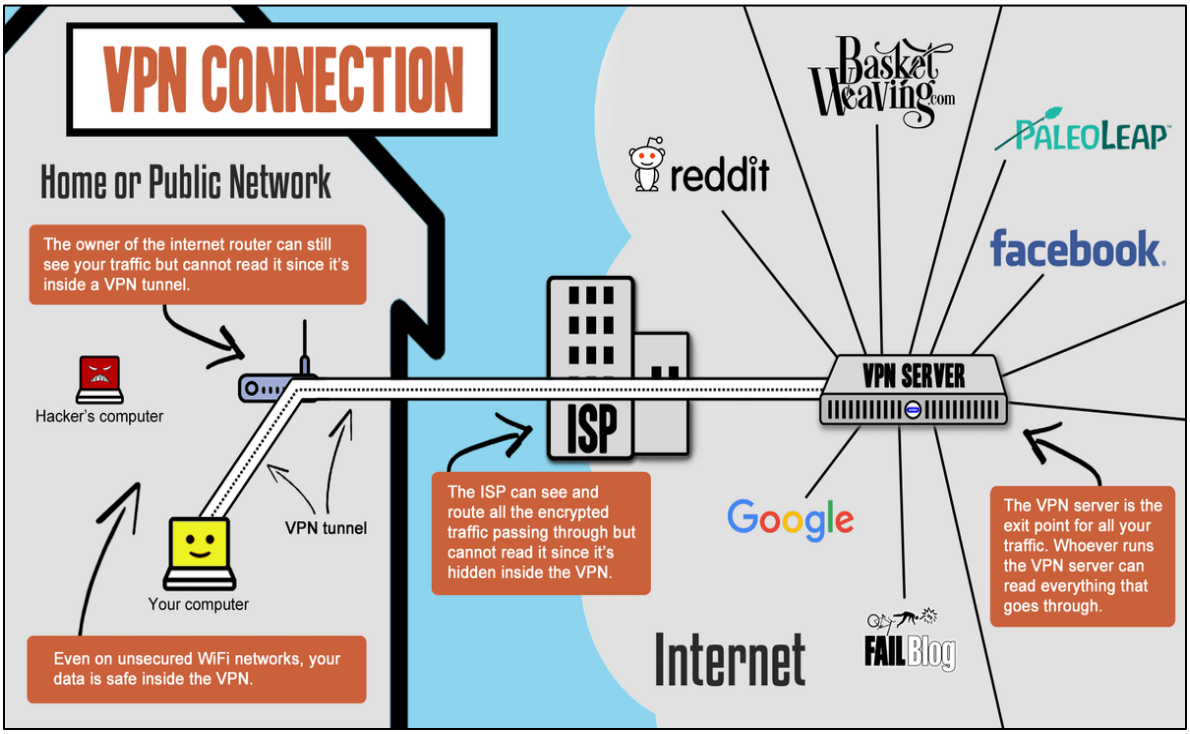

Figure 7 - VPN Connection Explanation

Appendix D - Man-In-The-Middle Attacks

Man-in-the-middle attacks occur when an individual gains access to web traffic as it passes between the recipient and the sender, allowing them to view the traffic from the recipient discretely. Without SSL certificates, this would be feasible and not too tricky. Today, it is uncommon to find a website that does not use SSL certification. See Figure 8 for an instance where a web page tells a user their website has an invalid SSL certificate. When this is on a webpage, be wary of the implications of not having an SSL Certificate, like having a third party access someone's unencrypted data.

Figure 8 - Invalid SSL certificate

Appendix E - Brute-Force attack

As the name depicts, brute-force attacks happen when an attacker forcefully attempts to gain passwords or other essential credentials. There are a variety of types of brute-force attacks, including:

- **Simple Brute-Force Attack** - When an attacker attempts to guess a person's username/password without using any software. Capitalizing on the most common passwords and PINs (i.e., password123, 1234, 4321), the attackers are banking on the user not having strong passwords. While simple brute force can be effective, there are far better methods of gaining credentials to a system.

- **Dictionary Attack** - Another basic form of attempting to gain credentials to a system. The attacker must know the username and then combines keywords with random numbers/letters to attempt to guess the password. EX: cowboys1, cowboys123, cowboys321. Similar to simple brute-force attacks, this process is extremely time-consuming and relatively ineffective.

- **Hybrid Brute-Force Attacks** - Occurs when an attacker combines simple brute-force and dictionary attacks. Like Dictionary attacks, hybrid brute-force attackers start with a username, use a list of potential words, and combine them with standard numbers or characters to find the correct password. Examples include europe123, elonmusksucks!1, and paradise10. The main difference between

Hybrid and Dictionary is that Hybrid focuses on common/popular words instead of taking a dictionary approach when brute-forcing a password.

- **Reverse Brute-Force Attacks -** This occurs when an attacker obtains a password, usually in a data leak, and attempts to match the password to an active login. Sometimes, the attackers use a simple password, such as password123, to comb through various usernames and see if they get any matches. While this can be effective, especially if an attacker already knows the password, most passwords get stored in hashes (Appendix I) instead of in plain text, so one is unable to see passwords being leaked like that usually.

- **Credential Stuffing -** Banking on the fact that the user reuses their passwords, credential stuffing occurs when an attacker obtains a password for their target and uses that password on other websites hoping that it is reused and will allow them access to the victims' systems.

Appendix F - Phishing / Spear Phishing Emails

Phishing

Phishing is one of the most common forms of cyber-attacks worldwide. Similar to fishing, one casts their bait & hook out to a vast sea of potential catches - Huge catfish, smaller trout, or sometimes nothing at all. Phishing does this by sending out mass emails to a wide variety of targets - like one casting their bait to a large lake or ocean - in hopes of one lucky target “taking a bite.” Phishers construct and deliver phishing emails using well-known companies like Google or Paypal to build a message they believe the recipient expects to receive. Examples include a new sign-on notification, monthly bills/reports, or anything related to the services they try to duplicate.

Once phishing emails appear in one's inbox, it is ultimately up to the receiver to determine if the attacker is successful. If the email ends up getting deleted, nothing happens. On the other hand, if the attackers successfully deceive the target into thinking the email originated from a legitimate source, they will ultimately end up clicking on the link, which infects them with malware. Malware can inflict a multitude of damage on the victims in various ways; holding one’s data for ransom, known as ransomware, or wiping hard drives clean. Sometimes, more commonly in spear phishing, they gain access to their system to observe and collect intelligence on the target's environment. The latter is more common with sophisticated attacks that require vast resources and planning and typically involve nation-states like Iran, North Korea, Russia, and the US.

Below is an email received from a Phisher, attempting to impersonate an email from Coinbase, a widely known website for transacting and storing cryptocurrency. Phishers typically mass-send emails to maximize their chances of success. As one can see below, the Phisher uses several techniques to disguise their email. First, they spoof the sender email to look like "From: no-reply@helpcoinbase.com," but in reality, it comes from "noreply@server08.cluhosting.com:"

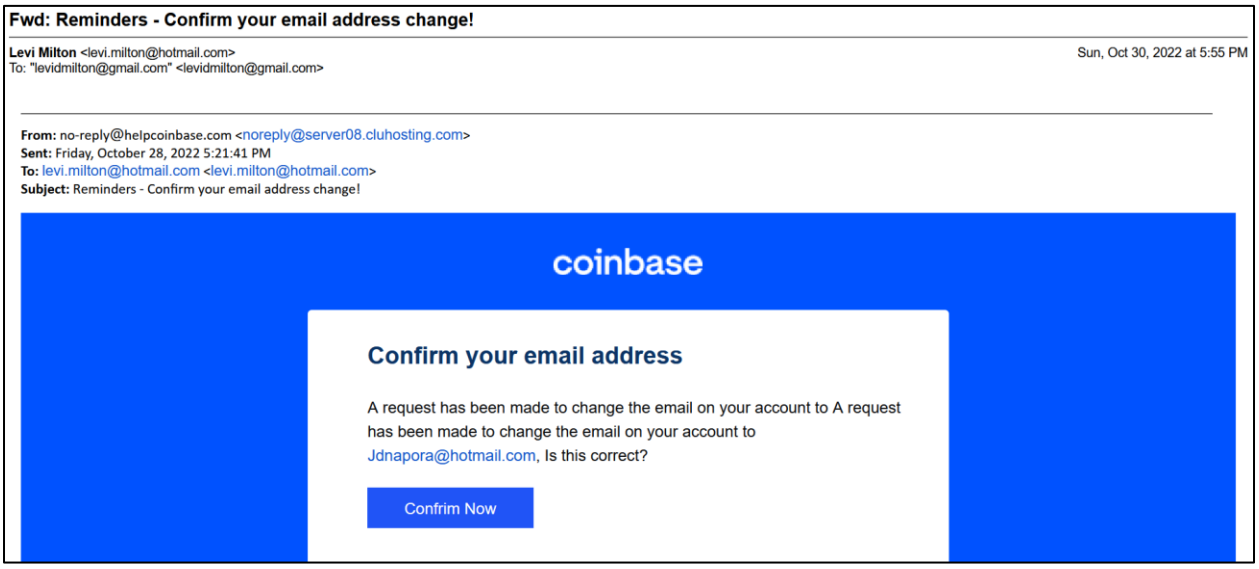

Figure 9 - Phishing Example

Second, in the Subject line, they curate it to mimic an email I would expect from Coinbase – one that confirms an email address change request. They were hoping to catch the victim in a state of surprise, thinking that someone was attempting to get into their account since they had not initiated an email change on their Coinbase account.

Third, notice the overall simplicity of the email they crafted. It looks like a kid made this message - there are misspellings, discrepancies in the logos used, lack of sophisticated grammar usage, and they even got the email wrong. Instead of levi.milton@hotmail.com,

they put Jdnapora@hotmail.com. These mistakes seem easy to fix, but according to some sources, they are intentional. Sometimes it is the lack of being a native English speaker, so they cannot accurately curate the email to match what we would expect to receive due to their lack of proficiency and familiarity with the English language. Lastly, and most probably, they are not targeting an average person but a more gullible, susceptible person who cannot notice the improper grammar and other mistakes mentioned above. By targeting these people, they are more likely to ensure success in infecting the victim's networks - usually the elderly. It is also a tactic to mitigate spam filters [34].

Spear Phishing (Figure 10)

Spear phishing is a sophisticated attack that uses phishing but targets a specific individual or segment of a business/organization. Instead of casting out a net or fishing line into a vast ocean, hoping to catch anything that bites, spear fishers must know where their target is. By understanding their prey and the target's actions, routine, and habits – they can target a specific fish. Similar to spearfishing in real life, one must dedicate a lot of time and expertise to get a “kill.”

Spear phishers stray from traditional phishing and approach a sophisticated method of attacking. They pick a target that usually has elevated privilege, such as an executive, and learn their daily routine, whom they email, what the emails entail, and what daily reports they get. By understanding this, they can curate their spear phishing email to mimic something that they might be expecting to receive. Phishers are even known to CC coworkers; while they are not the intended victims of the attack, attackers do this to help appear legitimate like the victim would expect to see on a daily routine.

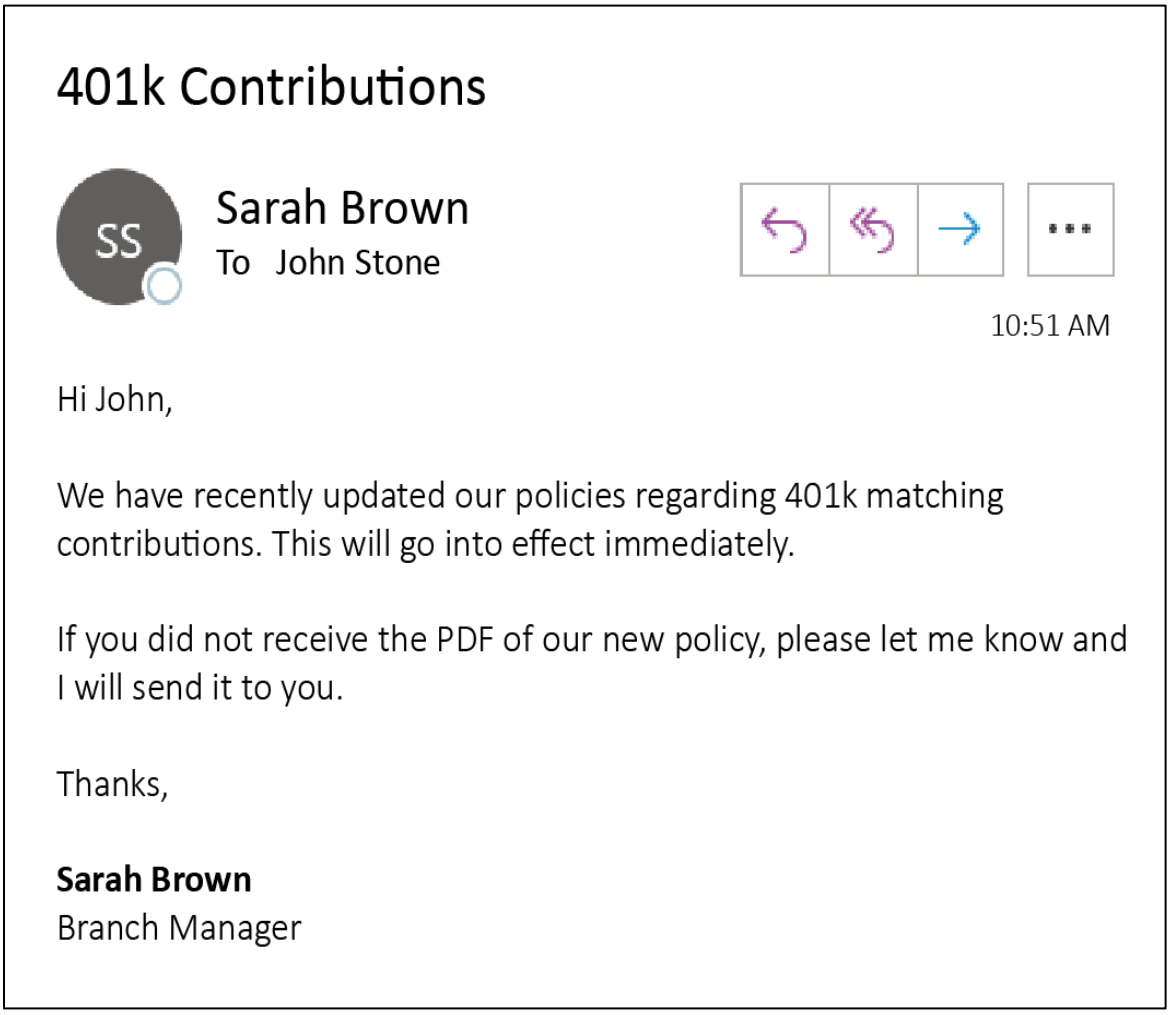

Figure 10 - Spear Phishing Example

This email appears to originate internally - Sarah Brown from HR asking about a new 401k Policy. The Phisher potentially knew that they were switching 401k policies and used this as an opportunity to spear phish. If the defender were unsuspecting, they would click on the PDF attached and download a virus in the process of doing so.

Appendix G - Wiper Malware

Wiper Malware is a form of malware that aims to erase the data on the infected system. It has come up in various attacks, including the 2012 Shamoon and 2014 Sony attacks, along with Ukraine since 2017. Wiper Malware usually works by deleting the Master Boot Record, which is the information that is first read from a hard drive when booting up. It tells the computer where Windows's location is on the hard drive so that Windows can launch accordingly from the correct files. If the Master Boot Record gets wiped, the drive cannot locate the copy of Windows (or any other Operating System) and becomes inoperable. Wiper malware is a highly effective method of ensuring that the systems are ineffective and without data.

Appendix H – Drivers

Drivers are a set of software whose goal is to communicate with the rest of the system. Specific to the parts and operating system, it communicates with the device via a “computer bus” connected to the hardware. When selecting a program, the driver sends a message to the device, and the device sends data back to the driver, allowing the program to run. While this is beneficial to ensure the longevity of the up-time on a system, it can offer another avenue for attackers to take when brainstorming how to infect their target system. Without drivers, the parts in our PC/systems cannot communicate. Because of this, Anti-Virus software does not scan active drivers due to their importance to the system's fluidity; if interrupted, it could be problematic to continue running the system.

Appendix I - Password Hashing

Password Hashing allows passwords and other private information to flow freely between servers without fear of inception by an outsider. When passwords are stored, (most) companies store these passwords in an encrypted hash. When the data becomes compromised, they are greeted with many letters and characters instead of seeing a plain-text password. Below is Figure 10, a simple chart explaining the process [58].

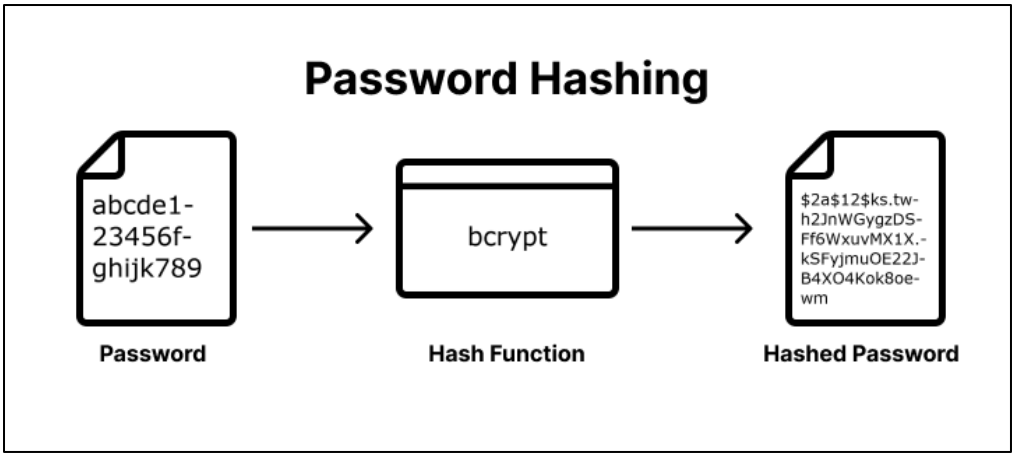

Figure 11 - Password Hashing

For example, the hash of 12345 is

5994471abb01112afcc18159f6cc74b4f511b99806da59b3ca.

While this offers an extra layer of encryption for one's passwords, hackers can still brute-force a password with only a hash by using algorithms to determine which hash matches what string of characters. With the release of the new Nvidia 4090 graphics card, it can crack any 8-digit password within 48 minutes [59].

Appendix J – COMODOHACKER's message on Pastebin

Hi again! I strike back again, huh?

I told all that I can do it again, I told all in interviews that I still have accesses in Comodo resellers, I told all I have access to most of CAs, you see that words now?

You know, I have access to 4 more so HIGH profile CAs, which I can issue certs from them too which I will, I won't name them, I also had access to StartCom CA, I hacked their server too with so sophisticated methods, he was lucky by being sitted in front of HSM for signing, I will name just one more which I still have access: GlobalSign, let me use these accesses and CAs, later I'll talk about them too..

I won't talk so many detail for now, just I wanted to let the world know that ANYTHING you do will have consequences, ANYTHING your country did in past, you have to pay for it...

I was sure if I issue those certificates for myself from a company, company will be closed and will not be able to issue certs anymore, Comodo was really really lucky!

I thought if I issue certs from Dutch Gov. CA, they'll lose a lot of money:

http://www.nasdaq.com/aspx/dynamic_charting.aspx?selected=VDSI&timeframe=6m&charttype=line

But I remembered something and I hacked DigiNotar without more thinking in anniversary of that mistake:

http://www.tepav.org.tr/en/kose-yazisi-tepav/s/2551

When Dutch government, exchanged 8000 Muslim for 30 Dutch soldiers and Animal Serbian soldiers killed 8000 Muslims in same day, Dutch government have to pay for it, nothing is changed, just 16 years has been passed. Dutch government's 13 million dollars which paid for DigiNotar will have to go DIRECTLY into trash, it's what I can do from KMs away! It's enough for Dutch government for now, to understand that 1 Muslim soldier worth 10000 Dutch government.

I'll talk technical details of hack later, I don't have time now... How I got access to 6 layer network behind internet servers of DigiNotar, how I found passwords, how I got SYSTEM privilage in fully patched and up-to-date system, how I bypassed their nCipher NetHSM, their hardware keys, their RSA certificate manager, their 6th layer internal "CERT NETWORK" which have no ANY connection to internet, how I got full remote desktop connection when there was firewalls that blocked all ports except 80 and 443 and doesn't allow Reverse or direct VNC connections, more and more and more...

After I explain, you'll understand how sophisticated attack it was, It will be a good hacking course for hackers like Anonymous and Lulzsec :) There was so many 0-day bugs, methods and skill shows...

Have you ever heard of XUDA programming language which RSA Certificate manager uses it? NO! I heard of it in RSA Certificate Manager and I learned programming in it in same night, it is so unusual like greater than sign in all programming languages is "<" but in XUDA it is "{"

Anyway... I'll talk about DigiNotar later! For now keep thinking about what Dutch government did in 16 years ago in same day of my hack, I'll talk later and I'll introduce to you MOST sophisticated hack of the year which will come more, you have to also wait for other CA's certificates to be used by me, then I'll talk about them too.

Interviews will be done via email ichsun [at] ymail.com

By the way, ask DigiNotar about this username/password combination:

Username: PRODUCTION\Administrator (domain administrator of certificate network)

Password: Pr0d@dm1n

It's not all about passwords or cracking them,

1) you can't have remote desktop connection in a really closed and protected network by firewalls which doesn't allow Reverse VNC, VNC, remote desktop, etc. by packet detection.

2) you can't even dump hashes of domain if you don't have admin privilege to crack them

3) you can't access 6th layer network which have no ANY connection to internet from internet

Yeah!

Bye for now

Appendix K – Cutting Sword of Justice's message on Pastebin

"We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action.

One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslim oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people.

In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours.

This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression. We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this

movement by designing and performing such operations, if they are against tyranny and oppression.

Cutting Sword of Justice" [27]

Appendix L – Donor list leaked from the DNC

	A	B	C
83	Morgan Freeman	$1,000,000.00	Los Angeles, CA
84	Mark Pincus	$1,000,000.00	San Francisco, CA
85	International Union Of Painters And Allied Trades Political Action Together Political Comm	$1,000,000.00	Washington, DC
86	Terry and Susan Ragon	$1,000,000.00	Cambridge, MA
87	Barbara Stiefel	$1,050,000.00	Coral Gables, FL
88	Steven Spielberg	$1,100,000.00	Los Angeles, CA
89	Michael Snow	$1,100,000.00	Wayzata, MN
90	S. Daniel Abraham	$1,200,000.00	West Palm Beach, FL
91	UAW Education Fund	$1,200,000.00	Washington, DC
92	National Air Traffic Controllers Association PAC	$1,250,000.00	Washington, DC
93	Mr. David E. Shaw	$1,375,000.00	New York, NY
94	Henry Laufer	$1,500,000.00	Lake Worth, FL
95	Ann Wyckoff	$1,500,000.00	Seattle, WA
96	American Federation of Teachers COPE	$1,500,000.00	Washington, DC
97	Anne Cox Chambers	$2,000,000.00	Atlanta, GA
98	Irwin Mark Jacobs	$2,000,000.00	La Jolla, CA
99	Jon Stryker	$2,000,000.00	New York, NY
100	United Association (Plumbers and Pipefitters) - incluing state/local checks they raised	$2,965,000.00	Annapolis, MD
101	Jeffrey Katzenberg	$3,000,000.00	Los Angeles, CA
102	Mr. J. Steve & Amber Mostyn	$3,003,850.00	Houston, TX
103	Fred Eychaner	$4,500,000.00	Chicago, IL
104	Mr. James H. Simons	$5,000,000.00	New York, NY
105			

References

[1] *Historic Personalities of Iran: Mohammad Reza Shah pahlavi*, 05-Dec-2022. [Online]. Available: https://www.iranchamber.com/history/mohammad_rezashah/mohammad_rezashah.php. [Accessed: 05-Dec-2022].

[2] UNESCO, "Literacy rate, youth male (% of males ages 15-24) - iran, Islamic rep.," *Data*, Jun-2022. [Online]. Available: https://data.worldbank.org/indicator/SE.ADT.1524.LT.MA.ZS?locations=IR. [Accessed: 05-Dec-2022].

[3] A. S. Cooper, *The Fall of Heaven: The pahlavis and the final days of Imperial Iran*. New York: Picador, 2018.

[4] D. Morgan, W. Pincus, and Washington Post Staff Writers; Researcher Valarie Thomas contributor to this article., "Iran's ambitions fed U.S. strategists, Weaponeers," *The Washington Post*, 13-Jan-1980. [Online]. Available: https://www.washingtonpost.com/archive/politics/1980/01/13/irans-ambitions-fed-us-strategists-weaponeers/12839d79-32e5-4849-a4d5-108a0aecab99/. [Accessed: 05-Dec-2022].

[5] M. Zonis, *Majestic failure: The fall of the shah*. Chicago: University of Chicago Press, 1991.

[6] S. Montag, “Black Friday: The massacre that ignited a revolution in Iran,” *Left Voice*, 09-Sep-2021. [Online]. Available: https://www.leftvoice.org/black-friday-the-massacre-that-ignited-a-revolution-in-iran/. [Accessed: 05-Dec-2022].

[7] “Iran Protests Shah's Move To Texas,” *Pittsburgh Post-Gazette*, Pittsburgh, 03-Dec-1979.

[8] K. Townsend, “The rise and fall of Ashiyane - Iran's foremost Hacker Forum,” *SecurityWeek*, 16-Jan-2019. [Online]. Available: https://www.securityweek.com/rise-and-fall-ashiyane-irans-foremost-hacker-forum. [Accessed: 01-Dec-2022].

[9] M. Kumar, *Website Defacement*. 2013.

[10] J. DiMaggio, “Chapter 1: Nation-State Attacks,” in *The art of cyberwarfare: An investigator's guide to espionage, ransomware, and organized cybercrime*, San Francisco: No Starch Press Inc, 2022, pp. 16–19.

[11] BBC, “Profile: Iran's revolutionary guards,” *BBC News*, 18-Oct-2009. [Online]. Available: http://news.bbc.co.uk/1/hi/world/middle_east/7064353.stm. [Accessed: 05-Dec-2022].

[12] A. Ward and N. Toosi, “Biden made final decision to keep Iran's IRGC on terrorist list,” *Biden made final decision to keep Iran’s IRGC on terrorist list*, 24-May-2022. [Online]. Available: https://www.politico.com/news/2022/05/24/biden-final-decision-iran-revolutionary-guard-terrorist-00034789. [Accessed: 01-Dec-2022].

[13] C. Stouffer, “What is an SSL certificate? A definition + FAQs answered,” *What is an SSL certificate?*, 08-Dec-2021. [Online]. Available: https://us.norton.com/blog/how-to/what-is-an-ssl-certificate#. [Accessed: 01-Dec-2022].

[14] “What is VPN? how it works, types of VPN,” *www.kaspersky.com*, 21-Oct-2022. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn. [Accessed: 05-Dec-2022].

[15] K. Zetter, “DigiNotar files for bankruptcy in wake of devastating hack,” *DigiNotar Files for Bankruptcy in Wake of Devastating Hack,* 20-Sep-2011. [Online]. Available: https://www.wired.com/2011/09/diginotar-bankruptcy/. [Accessed: 01-Dec-2022].

[16] “The last yugoslav census: Bosnia-Herzegovina's 1991 population ...” [Online]. Available: https://www.researchgate.net/figure/The-Last-Yugoslav-Census-Bosnia-Herzegovinas-1991-Population-according-to-Ethnicity_tbl1_231889150. [Accessed: 05-Dec-2022].

[17] “April 7, 1992: United States recognition of bih's independence,” *April 7, 1992: United States recognition of BiH’s Independence*, 07-Apr-2009. [Online]. Available: https://www.acbih.org/april-7-1992-united-states-recognition-of-bihs-independence/. [Accessed: 05-Dec-2022].

[18] E. Turbedar, *Srebrenica: 16 years later*, 11-Jun-2011. [Online]. Available: https://www.tepav.org.tr/en/blog/s/2551. [Accessed: 01-Dec-2022].

[19] “Srebrenica 1993-1995,” *United States holocaust memorial museum*. [Online]. Available: https://www.ushmm.org/genocide-prevention/countries/bosnia-herzegovina/srebrenica/violence/systematic-executions. [Accessed: 01-Dec-2022].

[20] “WRIT OF SUMMONS,” 2007. [Online]. Available: https://www.legal-tools.org/doc/ca1e99/pdf. [Accessed: 2022].

[21] VASCO Data Security International, “Prepared script of January 11, 2011 DIGINOTAR acquisition conference call,” *SEC*, 11-Jan-2011. [Online]. Available: https://www.sec.gov/Archives/edgar/data/1044777/000119312511008008/dex993.htm. [Accessed: 01-Dec-2022].

[22] VASCO Data Security International, *Form 8-K amendment*. [Online]. Available: https://www.sec.gov/Archives/edgar/data/1044777/000119312511263272/d239232d8ka.htm. [Accessed: 05-Dec-2022].

[23] K. Zetter, “DigiNotar files for bankruptcy in wake of devastating hack,” *Wired*, 20-Sep-2011. [Online]. Available: https://www.wired.com/2011/09/diginotar-bankruptcy/. [Accessed: 05-Dec-2022].

[24] COMODOHACKER, “Striking back...,” *Pastebin*, 05-Sep-2011. [Online]. Available: https://pastebin.com/1AxH30em. [Accessed: 01-Dec-2022].

[25] J. Wolff, “How a 2011 hack you've never heard of changed the internet's infrastructure,” *Slate Magazine*, 21-Dec-2016. [Online]. Available:

https://slate.com/technology/2016/12/how-the-2011-hack-of-diginotar-changed-the-internets-infrastructure.html. [Accessed: 01-Dec-2022].

[26] J. DiMaggio, “Chapter 1: Nation-State Attacks,” in *The art of cyberwarfare: An investigator's guide to espionage, ransomware, and organized cybercrime*, San Francisco: No Starch Press Inc, 2022, pp. 21-22.

[27] Cutting Sword of Justice, “Untitled,” *Pastebin*, 15-Aug-2012. [Online]. Available: https://pastebin.com/HqAgaQRj. [Accessed: 01-Dec-2022].

[28] R. Umoh, “This royal family's wealth could be more than $1 trillion ,” *CNBC*, 18-Aug-2018. [Online]. Available: https://www.cnbc.com/2018/08/18/this-royal-familys-wealth-could-be-more-than-1-trillion.html. [Accessed: 01-Dec-2022].

[29] Daily, “Top 10 companies in the world,” *Daily Logistics*, 13-Mar-2022. [Online]. Available: https://dailylogistic.com/top-10-companies-in-the-world/. [Accessed: 01-Dec-2022].

[30] J. Rackmill, “Maid Accuses Saudi Princess of Abuse,” *ABC News*, 18-Jan-2002. [Online]. Available: https://abcnews.go.com/2020/story?id=123950&page=1. [Accessed: 01-Dec-2022].

[31] M. Bröning, “Time to back the Syrian National Coalition,” *Foreign Affairs*, 08-Sep-2022. [Online]. Available: https://www.foreignaffairs.com/articles/syria/2012-12-17/time-back-syrian-national-coalition. [Accessed: 05-Dec-2022].

[32] J. McCallum, “Disk Prices 1965-present,” *Disk Drive prices 1955+*, 2022. [Online]. Available: https://jcmit.net/diskprice.htm. [Accessed: 05-Dec-2022].

[33] ARAMCO, “Saudi Aramco Annual Report 2012 - Saudi Aramco Annual Review 2012,” *ResourceData*, 2012. [Online]. Available: https://www.resourcedata.org/dataset/saudiaramco-annualreport-2012/resource/2902392f-57a9-4a5f-ae0f-bf70cad87235. [Accessed: 05-Dec-2022].

[34] B. J. Steinberg, “Why scammers make spelling and grammar ‘mistakes,’” *Joseph Steinberg: CyberSecurity Expert Witness, Privacy, Artificial Intelligence (AI) Advisor*, 02-Sep-2019. [Online]. Available: https://josephsteinberg.com/why-scammers-make-spelling-and-grammar-mistakes/. [Accessed: 05-Dec-2022].

[35] Cyber Security & Infrastructure Security Agency, “ICS Joint Security Awareness Report (JSAR-12-241-01B),” *CISA*, 16-Oct-2012. [Online]. Available: https://www.cisa.gov/uscert/ics/jsar/JSAR-12-241-01B. [Accessed: 05-Dec-2022].

[36] J. Strain, “Top 25 Richest People In The World 2014,” *Saving Advice*, 03-Mar-2014. [Online]. Available: https://www.savingadvice.com/articles/2014/03/03/1021201_top-25-richest-people-in-the-world-2014.html. [Accessed: 05-Dec-2022].

[37] P. Blumenthal, “Largest Republican Party donor wants to Nuke This Country,” *HuffPost*, 23-Oct-2013. [Online]. Available: https://www.huffpost.com/entry/sheldon-adelson-nuke-iran_n_4150237. [Accessed: 05-Dec-2022].

[38] J. Hoft, “Ayatollah Khamenei: US should slap Sheldon Adelson in the mouth,” *The Gateway Pundit*, 03-Nov-2013. [Online]. Available: https://www.thegatewaypundit.com/2013/11/ayatollah-khamenei-us-should-slap-adelson-in-the-mouth/. [Accessed: 05-Dec-2022].

[39] S. N. Nikou, “Timeline of Iran's nuclear activities,” *The Iran Primer,* 20-Aug-2021. [Online]. Available: https://iranprimer.usip.org/resource/timeline-irans-nuclear-activities. [Accessed: 05-Dec-2022].

[40] “Las Vegas sands market cap 2010-2022: LVS,” *Macrotrends*, 2022. [Online]. Available: https://www.macrotrends.net/stocks/charts/LVS/las-vegas-sands/market-cap. [Accessed: 05-Dec-2022].

[41] B. Elgin and M. Riley, “Iranian hackers hit Sheldon Adelson's sands casino in Las Vegas,” *Bloomberg.com,* 12-Dec-2014. [Online]. Available: https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas/. [Accessed: 05-Dec-2022].

[42] S. Gallagher, “Iranian hackers used visual basic malware to wipe Vegas Casino's network,” *Ars Technica*, 12-Dec-2014. [Online]. Available: https://arstechnica.com/information-technology/2014/12/iranian-hackers-used-visual-basic-malware-to-wipe-vegas-casinos-network/. [Accessed: 05-Dec-2022].

[43] T. Plattner, “Kim Jong-un stayed in Switzerland for nine years,” *LeMatin.ch*, 21-Apr-2012. [Online]. Available: https://www.lematin.ch/story/kim-jong-un-est-reste-neuf-ans-en-suisse-171219683893. [Accessed: 05-Dec-2022].

[44] J. White, “Dennis Rodman in North Korea: The adventures of an accidental ambassador,” *South China Morning Post*, 03-May-2020. [Online]. Available: https://www.scmp.com/sport/basketball/article/3082327/dennis-rodman-kim-jong-un-and-donald-trump-adventures-accidental. [Accessed: 05-Dec-2022].

[45] T. Claburn, “Cyber attack code starts killing infected pcs,” *Dark Reading*, 10-Jul-2009. [Online]. Available: https://www.darkreading.com/risk/cyber-attack-code-starts-killing-infected-pcs. [Accessed: 05-Dec-2022].

[46] J. DiMaggio, “Chapter 2: State-Sponsored Financial Attacks,” in *The art of cyberwarfare: An investigator's guide to espionage, ransomware, and organized cybercrime*, San Francisco: No Starch Press Inc, 2022, pp. 37-39.

[47] T. Branigan, “North Korea rocket launch provokes widespread condemnation,” *The Guardian*, 12-Dec-2012. [Online]. Available: https://www.theguardian.com/world/2012/dec/12/north-korea-rocket-launch-condemnation. [Accessed: 05-Dec-2022].

[48] Security Council, “Security Council condemns use of ballistic missile technology in launch by Democratic People's Republic of Korea, in Resolution 2087 (2013) | UN press,” *United Nations*, 2013. [Online]. Available: https://press.un.org/en/2013/sc10891.doc.htm. [Accessed: 05-Dec-2022].

[49] “A heist to remember: Three scandals that remain unsolved,” *Cyber Magazine*, 17-Aug-2022. [Online]. Available: https://cybermagazine.com/articles/a-heist-to-remember-three-scandals-that-remain-unsolved. [Accessed: 05-Dec-2022].

[50] J. DiMaggio, “Chapter 2: State-Sponsored Financial Attacks,” in *The art of cyberwarfare: An investigator's guide to espionage, ransomware, and organized cybercrime*, San Francisco: No Starch Press Inc, 2022, pp. 45-51.

[51] E. Caesar, “The incredible rise of north korea's Hacking Army,” *The New Yorker*, 19-Apr-2021. [Online]. Available: https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army. [Accessed: 05-Dec-2022].

[52] D. Hall, “Inside Kim Jong-un's lavish lifestyle from private palaces to millions blown on lingerie for his 'pleasure squad',” *The US Sun*, 30-Apr-2021. [Online]. Available: https://www.the-sun.com/news/759895/kim-jong-un-north-korea-lifestyle-palaces/. [Accessed: 05-Dec-2022].

[53] J. DiMaggio, “Chapter 2: State-Sponsored Financial Attacks,” in *The art of cyberwarfare: An investigator's guide to espionage, ransomware, and organized cybercrime*, San Francisco: No Starch Press Inc, 2022, pp. 52-54.

[54] Threat Hunter Team, *How the Lazarus Group is Emptying Millions from ATMs*. 2018.

[55] J. DiMaggio, “Chapter 4: Election Hacks,” in *The art of cyberwarfare: An investigator's guide to espionage, ransomware, and organized cybercrime*, San Francisco: No Starch Press Inc, 2022, pp. 88-89.

[56] M. Slack, “President Obama announces New Ukraine-related sanctions,” *National Archives and Records Administration*, 17-Mar-2014. [Online]. Available: https://obamawhitehouse.archives.gov/blog/2014/03/17/president-obama-announces-new-ukraine-related-sanctions. [Accessed: 05-Dec-2022].

[57] “Chapter 1 - Collusion,” *The Moscow Project*, 2022. [Online]. Available: https://themoscowproject.org/collusion-chapter/chapter-1/index.html. [Accessed: 05-Dec-2022].

[58] “Password hashing and Salting explained,” *Authgear*, 07-Apr-2022. [Online]. Available: https://www.authgear.com/post/password-hashing-salting. [Accessed: 05-Dec-2022].

[59] D. James, “8 RTX 4090s could crack most of your passwords in just 48 minutes,” *pcgamer*, 18-Oct-2022. [Online]. Available: https://www.pcgamer.com/just-8-rtx-4090s-could-crack-most-of-your-passwords-in-48-minutes/. [Accessed: 05-Dec-2022].

[60] J. DiMaggio, “Chapter 4: Election Hacks,” in *The art of cyberwarfare: An investigator's guide to espionage, ransomware, and organized cybercrime*, San Francisco: No Starch Press Inc, 2022, pp. 93-101.

[61] Guccifer2, “Guccifer 2.0 DNC's servers hacked by a lone hacker,” *GUCCIFER 2.0*, 16-Jun-2016. [Online]. Available: https://guccifer2.wordpress.com/2016/06/15/dnc/. [Accessed: 05-Dec-2022].

[62] U.S NRC, “Uranium enrichment | nrc.gov,” 02-Dec-2020. [Online]. Available: https://www.nrc.gov/materials/fuel-cycle-fac/ur-enrichment.html. [Accessed: 06-Dec-2022].

[63] J. DiMaggio, “Chapter 1: Nation-State Attacks,” in *The art of cyberwarfare: An investigator's guide to espionage, ransomware, and organized cybercrime*, San Francisco: No Starch Press Inc, 2022, pp. 24-26.

[64] J. Kopfstein, “Stuxnet virus was planted by Israeli agents using USB sticks, according to New Report,” *The Verge*, 12-Apr-2012. [Online]. Available: https://www.theverge.com/2012/4/12/2944329/stuxnet-computer-virus-planted-israeli-agent-iran. [Accessed: 06-Dec-2022].

[65] “Iran blames U.S., Israel for stuxnet malware,” *CBS News*, 16-Apr-2011. [Online]. Available: https://www.cbsnews.com/news/iran-blames-us-israel-for-stuxnet-malware/. [Accessed: 06-Dec-2022].