The Nature of Phishing and Payload Delivery

Broderick Wolff[1], Alexander Hughes[2], Xin Wang[3], Kanwal Gagneja[4]
[1,2,3,4]Florida Polytechnic University, Lakeland, FL, United States
[1]broderickwolff0714@floridapoly.edu, [2]ahughes3300@floridapoly.edu, [3]xwang2945@floridapoly.edu,
[4]kgagnej@floridapoly.edu

Abstract:
In this modern age of digital technology, it comes as no surprise that one of the most concerning developments in the world is the rate at which cybercrime is growing and evolving. The inherent esoteric nature of cybercrime combined with a level of anonymity known only through online interaction has created an environment for criminals to trial and perfect new means of stealing information and causing havoc. Phishing, the practice of malicious online entities masquerading as legitimate services with the intent of stealing information, has become one of the most prolific cybercrimes of the era. In this paper, we aim to discuss the nature of phishing and the various methods different groups and attackers have employed over the years. We also intend to dissect these fraudulent activities through trials of our own in hopes of better understanding the overall process.

Keywords: Phishing, payload, hacking, cybercrime, threat.

1. Introduction

The ubiquity of the internet and related technologies in today's society means that we now live in a world where exchanging large sums of information over long distances is no longer an arduous task [22]. Gone are the days of requiring a local library to look up specific topics, as are the years of dealing with banks exclusively in person. In place of these things, we now have computers and smart devices readily available to us, making the processes of communicating with others and sharing information easier than ever [21] [27]. The power of the world's largest information network is readily available at one's fingertips through modern technological marvels [7]. Millions of people worldwide are now capable of carrying out a significant portion of their daily lives entirely through the internet, making it simultaneously the most influential and terrifying advancement of this modern era.

With such a massive amount of our daily routines moving over to the internet, it is only expected that other aspects of our lives have transitioned over to it, as well. One of the most concerning developments of the last several decades is the emergence and development of cybercrime, or criminal activity entirely unique to the digital era. The continued advocation of internet use and the rapid development of any and all associated technologies has fueled the growth of cybercrime, resulting in much more sophisticated and impactful forms of malicious activity.

One of the more insidious and far reaching cybercrime techniques in use today is commonly referred to as phishing. Traditionally, phishing refers to the practice of soliciting responses from targets through fraudulent means such as email scams [19] [26]. The attacker impersonates a legitimate service during interactions with a target, encouraging them to respond with information that they otherwise would not share. While this type of criminal exercise may not be as immediately eye-catching as other activities such as Hollywood's depictions of hacking, phishing is not only a serious threat, but one of the most prolific forms of digital crime altogether.

Above all else, phishing is at its most dangerous when considering the implications of the attack structure itself. Phishing scams can potentially target millions of users of varying backgrounds, all while targeting different individuals for various reasons. Some scams may end at obtaining personal credentials regarding finances, whereas others may simply be means of gaining access to private systems. Phishing scams are often employed as means of delivering malicious payloads to aid in committing other cybercrimes. According to Symantec's 2017 Internet Security Threat Report (ISTR), 1 in 131 emails contained malware in 2016, the highest rate in five years. [1]

In this paper, we have proposed a technique to crack phishing. First, we intend to review the different methods commonly employed by attackers to carry out phishing scams as well as the means organizations and forensics teams employ to prevent and crack down on this form of criminal activity. We also seek to review our own sample data involving a small-scale trial for delivering a malicious payload through a phishing scam. Finally, we build our own malicious payload to gain valuable insight in various forms of malware functionality.

2. Phishing Methods

While phishing is often referenced as a single attack type, there are actually a number of different methods commonly employed by attackers in order to accomplish different goals. In this section, we will discuss the most common and relevant attack types and their implications.

2.1. Email Spam

Without a doubt, email spam is the most commonly cited form of phishing used by attackers. According to the IBM Threat Intelligence Index for 2017, the overall volume of spam emails increased 4x in 2016, with over half of all emails sent being malicious spam [2].Most forms of email spam will issue a common format, such as banking or other user forms, to millions of users in an attempt to reach a broad demographic of users within a single group. For example, email scams structured to reflect social media emails or tax return forms are commonly used to trick

unknowing users into offering personal credentials to attackers [12]. These scams can escalate in impact rapidly, as they may offer attackers means of transitioning into other criminal endeavors such as identity theft and malware distribution [23].

2.2. Spear Phishing

While traditional phishing such as broad email spam offers wide coverage to an attacker, spear phishing is a much more organized and targeted approach to employing a scam [14]. Spear phishing, as its namesake implies, is the act of selectively identifying and pursuing a specific target for an attack. In most cases, attackers will study their target, be it a single individual or members of an organization, and issue an attack geared specifically for their needs. These attacks are often heavily personalized for specific groups and companies as a means of capitalizing on assumed factors in their routines, increasing the likelihood that an attack will be successful.

2.3. Malware

While not a form of phishing itself, malware plays an integral role in phishing. Malware, any software designed for malicious purposes, is a key player in many widespread phishing scams, enabling a level of sophistication to attackers that would otherwise be impossible without it [13] [17]. Whether through email attachments or fraudulent websites acting as payload centers, malware can increase the destructive impact of a phishing attack exponentially. Keyloggers, malware that tracks keyboard inputs, are commonplace payloads that are often used to obtain personal information without the user's knowledge. Trojans purporting legitimate files and applications create security risks for users and means of access for attackers. Ransom ware, a growing cybercrime tactic in and of itself, is a form of malware that denies access to files and/or devices until a ransom has been paid in full [9]. These are some of the most popular forms of malware used today, especially in the context of phishing scams.

2.4. Link Manipulation

Often employed in conjunction with email spam, link manipulation is a fairly popular tactic used by scammers to draw traffic to malicious websites and services [18]. These links are often disguised by fraudulent forms and emails that encourage users to follow them to fake websites and payload centers. These links are often part of multilayered scams, drawing traffic through popular email formats and occasionally public forums.

2.5. Malicious Advertising

One growing trend in the realm of cybercrime is the development and implementation of malicious advertisements. Unlike the adware of the years prior, which were payloads that forced browsers to show specific content, malicious advertising or "malvertising" is a delivery method rather than a payload itself. The tactic involves active scripts taking advantage of security flaws through internet browsers to force unwanted content onto your device. This method of delivery can be especially insidious, as it requires no security risk through a website itself. Legitimate websites running suspicious ads can subject their user bases to malvertising if they are not careful.

2.6. Website Fraud

One of the most dangerous forms of phishing, website fraud is an incredibly broad and potentially complicated form of phishing growing in popularity. Often employed in multilayered phishing scams, website fraud can be described as a website masquerading as a legitimate service to entice users to enter personal credentials. These websites are often part of email scams as means of offering more visual legitimacy to the scams. Unlike email spam, however, these websites can capitalize on a number of security vulnerabilities and deployment methods outside of spam. Websites can take advantage of search engine queries to return as results to broad or niche searches, gaining traffic outside of spam endeavors. Websites can also employ tactics such as malicious advertising to force malicious payloads onto unsuspecting users.

During our research, we personally took note of what we perceived to be an increasing trend of website fraud targeting users of piracy networks [8]. While users of these services are already subjecting themselves to certain risks, we feel that the development of these newer fraud-based vulnerabilities were worth acknowledging. In the case of commonplace torrent index networks like The Pirate Bay and its derivatives, there seems to be an increase in websites that seek to redirect traffic from common outlets to their own index listings [25]. While these websites do offer the same functionality as the commonplace websites, they do so while exposing users to vulnerabilities such as malicious advertising and other script activity.One specific piracy index known as the Kiss network has been fervently targeted by attackers as of late. A number of duplicate websites have emerged over the last year attempting to direct traffic away from the actual network in order to expose users to malicious ads as they traverse the otherwise functional fake website [11]. What makes these fraud piracy sites so much more dangerous than websites impersonating legal services is the low power and presence they have through search engines. Unlike real services, these websites do not command the same level of traffic or acknowledgement from search engines as higher profile websites do, allowing duplicates to hold just as much or more presence than the originals in search queries.

3. Forensics Techniques

Phishing is one of the most prevalent forms of cybercrime in this digital era. In 2016, 60% of enterprises were victims of social engineering attacks such as phishing emails [3]. Of those 60% of attacked enterprises 65% of the attacks resulted in employee credentials being leaked and 17% resulted in financial and client data being compromised [4].

Forensic techniques start with the email itself. Studying how the email was written and how it was able to infiltrate system is important. Sometimes phishing emails require the user to download a file and execute it or click on a link to webpage. The forensic investigator can use these pieces of information to understand the attack. Tools such as FTK imager can be used to create a bit-stream image of the files in question [5]. Email forensics also involves checking out the networks from which the email originated from and tracing route the message took to get to the receiver. In the case of a webpage being used the host can be contacted and possibly subpoena to give account information [6]. Another useful tool is a website set up specifically set up to stop phishing emails www.phishtank.com. This website is a database of reported phishing emails and can help an investigator identify a common phishing email. It is important for companies to adopt strict policies to help prevent such attacks from happening. These policies involve not opening strange emails, attachments or links to external pages and for employees to report any suspicious emails to their security teams.

Test Cases - 2

Equipped with the knowledge of various phishing methods, we set out to structure our own phishing scam in an attempt to better understand methods of entrapping users and deploying malicious content. For the sake of scalability, we chose to create a set of email scams for ease of implementation and testing.

For our first trial, we gathered a small sample of 160 students at Florida Polytechnic University. For the sake of privacy concerns, we have chosen to have these participants remain anonymous [10]. These students agreed to accept part in experiencing a mock phishing scam firsthand, allowing us to send spam attempts to their school inboxes in any manner we desired. The information provided to participants was as follows:

1. All phishing attempts will occur within five weeks of the starting date.
2. The scam will be e-mail oriented, targeting school e-mail specifically.
3. The attack will not exploit any local system security vulnerabilities. Any payload related materials will be purely for example purposes and will not be malicious or remotely executed.

While this information significantly aids our sample group in terms of protection, we withheld the following information to our benefit for testing:

1. The participants are unaware of the total number of targets of this attack.
2. The participants are unaware of how many attempts will be made during the testing period.
3. The targets are unaware of how broad or specific the attack plan is.

With these things in mind, we believed that the sample environment crafted would reasonably emulate a live environment of targets with moderate awareness of phishing and their status as potential targets.

Trial 1

For our first trial, we structured a simple broad email scam claiming to ask students to follow a link to a surveyabout course offerings. The link itself was a disguised live Dropbox link to our payload delivery method, initiating a download upon being contacted. We carried out this attempt within days of starting the entire process, giving the participants ample reason to suspect foul play immediately.

The results were fairly predictable, with only ten individuals confirming that they fell for and responded to the scam. We knew it was incredibly unlikely that this initial attempt would see greater success given the heightened awareness of the sample group in conjunction with the thinly veiled phishing attempt.

Trial 2

Our next trial, while very similar to the first; a simple email scam geared towards students with a disguised live link to our payload delivery method. However, the scam differed in two critical ways. For starters, we waited for nearly three weeks following the first trial to begin the next trial. Second, this trial would capitalize on current, relevant events within the student body. Specifically, the scam was structured to look like a mass email to Florida Polytechnic students offering their annual free tickets to an upcoming school convention, an annual occurrence that our sample group would be aware of. This difference gave the second trial a drastic advantage over the first; whereas the first trial was geared toward students, the second trial better reflected spear phishing attempts that capitalize on personal information and circumstance.

The results were far more intriguing than the first trial, with 130 out of 160 students falling victim to the scam within days of it being issued. Of these students, eighty admitted to clicking the link immediately without verifying the integrity of the email due to the specific nature of the information provided. One participant admitted to actually noticing the suspicious outgoing link prior to clicking it, but followed the link anyway after convincing themselves that it was likely just a different means to distributing tickets.

Analysis

The first thing we noticed is the difference between the results of the first trial and the second trial. We went into these tests knowing fully well that the results of the second trial would likely see more victims in our sample, but the difference is rather significant. Ignoring the two differing topics and layouts, the two trials were functionally the same scam. Even so, one of these trials vastly outperformed the other with such minor changes.

Due to the nature and scale of the tests we ran during our research, we cannot definitively say for certain that our results are the most accurate representation for largescale scams. With this in mind, we still feel that our tests reflect just how vulnerable people can be when they assume security through familiarity; all it took was the inclusion of personalized information to convince the once wary victims of our email's legitimacy.

4. Payload Description

In our research, we emulated an attack on our own systems in an effort to better understand how such attacks work. First, the victim of the attack is tricked into downloading a malicious executable file hosted by an online service such as drop box. This is done by setting up a direct download link to the file on drop box. The executable is named and disguised to resemble a different program such as canvas.exe. The file has to be downloaded through a service like drop box to circumvent protections in the Florida Poly email system that filters out executable files. The steps our virus takes through an infection is as follows:

Step 1

The first thing the virus does is scan the computer and creates a tree of all the directories present on the victim computer as shown in fig. 1. This is saved in a file named path.txt.

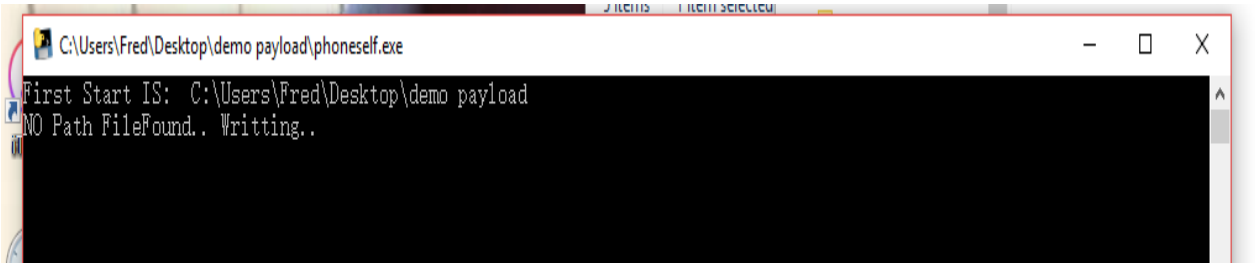

Fig. 1. tree of all the directories is created

Step 2

The virus then jumps to a random directory found in the path.txt file and replicates itself there then deletes the previous copy as shown in fig. 2. The virus does this to help make itdifficult to locate and eliminate the virus file. This replication repeats again after a short listening period.

```
C:\iverilog\lib\tcl8.5\tzdata\Arctic
C:\iverilog\lib\tcl8.5\tzdata\Asia
C:\iverilog\lib\tcl8.5\tzdata\Atlantic
C:\iverilog\lib\tcl8.5\tzdata\Australia
C:\iverilog\lib\tcl8.5\tzdata\Brazil
C:\iverilog\lib\tcl8.5\tzdata\Canada
C:\iverilog\lib\tcl8.5\tzdata\Chile
C:\iverilog\lib\tcl8.5\tzdata\Etc
C:\iverilog\lib\tcl8.5\tzdata\Europe
C:\iverilog\lib\tcl8.5\tzdata\Indian
C:\iverilog\lib\tcl8.5\tzdata\Mexico
C:\iverilog\lib\tcl8.5\tzdata\Pacific
C:\iverilog\lib\tcl8.5\tzdata\SystemV
C:\iverilog\lib\tcl8.5\tzdata\US
C:\iverilog\lib\tk8.5
C:\iverilog\lib\tk8.5\demos
C:\iverilog\lib\tk8.5\demos\images
C:\iverilog\lib\tk8.5\images
C:\iverilog\lib\tk8.5\msgs
```

Fig. 2. Random directory in path.txt file

Step 3

The virus then enters a ready state and waits for a command to be sent to it. The commands are sent via text messages through a service called bandwidth which allows sms text messages from cell phone to be sent to a computer connected to the internet.Fig. 3 represents the information returned when the path command is given. This returns the current directory the virus is in.

Step 4

A command is sent to the virus. After receiving a command, the virus executes the associated function that was programed into the virus. The following is a list of command functions programmed into the virus.

List of Commands

1) dir – This shows all the subdirectories of the directory that virus is currently residing.
2) path – Shows the directory location that virus currently resides in.
3) stop – This stops the replicating step of the virus.

Fig. 3. information returned when path command is given

4) continue – Starts up the replicating process of the virus after having been previous stopped.
5) cam – Captures an image from the computer's camera.
6) screen – Captures a screenshot image from the computer.
7) exit – Kills the virus process on the system.

Code Structure

The code structure of the virus is fairly simple. The virus itself is divided into two separate classes. The first class is called selfReplicate and contains all the functions for replicating the virus and functions for the various commands the virus receives.It is shown in figure 4. The second class is called listener as shown in figure 5 and contains the functions for listening to the network for incoming commands which in then returns to the selfReplicate class where the appropriate command function is executed. The code includes system exploits to better hide the executable file, optimizing the program for faster executions and improved precision of the functions themselves.

```
class selfReplicate():
        def __init__(self):
                self.root = os.path.abspath(os.sep)
                #self.root = "C:/Users/Fred/Desktop/
                self.trySetRoot()
                self.remove()
                self.read() #inialize self.f
                self.run()
```

Fig.4.Class selfreplicate

```
class Listener():
        def __init__(self):
                self.commandList = {"STOP": 0, "EXIT":1, "DIR": 2, "PATH": 3, "CONTINUE": 4, "SCREEN": 5, "CAM":6}


        def getTimeList(self):
                tempTime = datetime.today().replace(microsecond=0) + timedelta(hours = 4) + timedelta(seconds = -30) #thi
                startMessageList = list(messaging_api.list_messages(direction="in", size=1000, from_date_time =tempTime))
                return startMessageList


        def listening(self, pMessID):
                command = None
                timeList = self.getTimeList()
                #print("ACCEPTED ID: ", pMessID)

                if (len(timeList) > 0):
                        if timeList[0]["text"].upper() in self.commandList:
                                command = timeList[0]["text"].upper()
                        else:
                                command = timeList[0]["text"]
                        if pMessID == "None": #for loop goes through all the messages in list to send
                                pMessID = timeList[0]["id"]
                        else:
                                if pMessID == timeList[0]["id"]:
                                        #print("IM THE SAMMMEE", pMessID)
                                        command = None
                                else:
                                        #print("im not the same", pMessID)
                                        pMessID = timeList[0]["id"]

                return command, pMessID
```

Fig.5.Class Listener

5. Conclusion

Phishing is definitively one of the most impactful forms of cybercrime to emerge with the widespread adoption of the internet. As users continue to place their trust and various aspects of their livelihood in online activities, phishing scams will continue to appear and evolve. Cybercrime has come a long way over the last several decades, with a multitude of different attack methods having evolved drastically in complexity as the years passed. Phishing itself encompasses a plethora of attack methods that have grown far beyond the initial endeavor of spam emails. A combination of website fraud, malicious advertising, and various other methods discussed in this paper all offer evidence pointing towards an overall growth in sophistication within the phishing process itself.

There is a lot to be said for the measures taken by modern attackers and their efforts to stay several steps ahead of users and analysts alike. It is with this in mind that those

who desire to stop them must better understand their methods by studying how attacks are carried out. During our research, we covered the most popular attack types in detail to grasp just how in depth these phishing scams really are. Through our test case, we were able to apply the knowledge in order to carry out our own phishing attempts and gained valuable insight on some key differences between attack vectors. Finally, through designing and implementing our own malicious payload, we showed that by just changing the outlook of the application can influence the user to hit the wrong link.

Our goal during for this study was to cover all prominent avenues for phishing and apply it. We took our knowledge of attack vectors and applied it in our trials, seeing firsthand how the precision offered through spear phishing methods can yield drastically different results when used correctly against primed targets. We also explored the different functions of a malicious payload and associated delivery methods in order to learn of the possibilities available to attackers and the vulnerabilities to be exploited.

REFERENCES

[1] Symantec. (2017). 2017 Internet Security Threat Report. Retrieved March 8, 2018, from https://www.symantec.com/security-center/threat-report

[2] IBM Security. (2017). Threat Intelligence Index 2017. Retrieved March 9, 2018, from https://www.ibm.com/security/data-breach/threat-intelligence

[3] KnowBe4. (2015, Fall). Phishing Techniques. Retrieved March 11, 2018, from http://www.phishing.org/phishing-techniques

[4] Perez, R. (30, November 2016). 60% of enterprises were victims of social engineering attacks in 2016. Retrieved April 2, 2018, from https://www.scmagazineuk.com/ 60-of-enterprises-were-victims-of-social-engineering-attacks-in-2016/article/576060/

[5] Amrit, C. (2015, December 09). CASE STUDY: Website Phishing Attack. Retrieved April 5, 2018, from https://www.cybrary.it/0p3n/case-study-website-phishing-attack/

[6] K. Kaur, X. Xiaojiang Du and K. Nygard, “Enhanced routing in Heterogeneous Sensor Networks”, IEEE Computation World’09, pp. 569-574, Athens, Greece, Nov. 15-20, 2009.

[7] Lauren Evanoff, Nicole Hatch, Gagneja K.K., “Home Network Security: Beginner vs Advanced”, ICWN, Las Vegas, USA, July 27-30, 2015.

[8] Gagneja K.K. and Nygard K., "Heuristic Clustering with Secured Routing in Heterogeneous Sensor Networks", IEEE SECON, New Orleans, USA, pages 51-58, June 24-26, 2013.

[9] Gagneja K.K., “Knowing the Ransomware and Building Defense Against it - Specific to HealthCare Institutes”, IEEE MobiSecServ, Miami, USA, pp. 1-5, Feb. 11-12, 2017.

[10] Gagneja K.K., “Secure Communication Scheme for Wireless Sensor Networks to maintain Anonymity”, IEEE ICNC, Anaheim, California, USA, pp. 1142-1147, Feb. 16-19, 2015.

[11] Gagneja K.K., "Pairwise Post Deployment Key Management Scheme for Heterogeneous Sensor Networks", 13th IEEE WoWMoM 2012, San Francisco, California, USA, pages 1-2, June 25-28, 2012.

[12] Gagneja K.K., “Global Perspective of Security Breaches in Facebook”, FECS, Las Vegas, USA, July 21-24, 2014.

[13] Gagneja K.K., "Pairwise Key Distribution Scheme for Two-Tier Sensor Networks", IEEE ICNC, Honolulu, Hawaii, USA, pp 1081-1086, Feb. 3-6, 2014.

[14] Gagneja K., Nygard K., "Energy Efficient Approach with Integrated Key Management Scheme for Wireless Sensor Networks", ACM MOBIHOC, Bangalore, India, pp 13-18, July 29, 2013.

[15] Gagneja K.K., Nygard K., "A QoS based Heuristics for Clustering in Two-Tier Sensor Networks", IEEE FedCSIS 2012, Wroclaw, Poland, pages 779-784, Sept. 9-12, 2012.

[16] K. K. Gagneja, K. E. Nygard and N. Singh, "Tabu-Voronoi Clustering Heuristics with Key Management Scheme for Heterogeneous Sensor Networks", IEEE ICUFN 2012, Phuket, Thailand, pages 46-51, July 4-6, 2012.

[17] Gagneja K.K., Nygard K., "Key Management Scheme for Routing in Clustered Heterogeneous Sensor Networks", IEEE NTMS 2012, Security Track, Istanbul, Turkey, pp. 1-5, 7-10 May 2012.

[18] Runia Max, Gagneja K.K., “Raspberry Pi Webserver”, ESA, Las Vegas, USA, July 27-30, 2015.

[19] A. S. Gagneja and K. K. Gagneja, "Incident Response through Behavioral Science: An Industrial Approach," 2015 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, 2015, pp. 36-41.

[20] Tirado E., Turpin B., Beltz C., Roshon P., Judge R., Gagneja K., “A New Distributed Brute-Force Password Cracking Technique”, Future Network Systems and Security, FNSS Communications in Computer and Information Science, vol. 878, pp 117-127, 2018

[21] Caleb Riggs, Tanner Douglas and KanwalGagneja, "Image Mapping through Metadata," Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 2018, pp. 1-8.

[22] Keely Hill, Gagneja K.K., “Concept network design for a young Mars science station and Trans-planetary communication", IEEE MobiSecServ 2018, Miami, FL, USA, Feb. 24-25, 2018.

[23] Javier Campos, Slater Colteryahn, GagnejaKanwal, “IPv6 transmission over BLE Using Raspberry PI 3", International Conference on Computing, Networking and Communications, Wireless Networks (ICNC'18 WN), March 2018, pp. 200-204.

[24] Gagneja K., Jaimes L.G., “Computational Security and the Economics of Password Hacking”, Future Network Systems and Security. FNSS 2017. Communications in Computer and Information Science, vol. 759, pp. 30-40, Springer, 2017.

[25] Gagneja K.K. Ranganathan P., Boughosn S., Loree P. and Nygard K., "Limiting Transmit Power of Antennas in Heterogeneous Sensor Networks", IEEE EIT2012, IUPUI Indianapolis, IN, USA, pages 1-4, May 6-8, 2012.

[26] C. Riggs, J. Patel and K. Gagneja, "IoT Device Discovery for Incidence Response," 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 2019, pp. 1-8.

[27] S. Godwin, B. Glendenning and K. Gagneja, "Future Security of Smart Speaker and IoT Smart Home Devices," 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 2019, pp. 1-6.