CYFIRMA
DECODING THREATS

ADVANCED SOCIAL ENGINEERING ATTACKS DECONSTRUCTED

EXECUTIVE SUMMARY

The team at CYFIRMA has analyzed and researched social engineering attacks in depth. The research paper reports techniques used by various threat actors to initiate the first stage of a deadly cyber-attack. The paper discusses the psychological role, and how it becomes an important part of the social engineering attack. Further, we discuss a few social engineering attacks which led to successful compromises. This paper will expose the mindset that drives threat actors to plan and execute social engineering attacks on various occasions.

ABSTRACT

CYFIRMA will break down each part of social engineering attacks from the attacker's perspective as part of this research. We will discuss and study the attacker's approach to social engineering attacks as per long and short-term goals. This should help users to gain clear awareness of social engineering attacks that are planned by the threat actors behind closed doors. All the bigger and smaller cyber-attacks are led by social engineering. Plucking the first step of a cyber-attack from the root level would help cyberspace to be more secure. This paper will have a detection section to help the cyber community identify potential attacks before they could even start.

INTRODUCTION

Social engineering attacks psychologically manipulate the human mind and make them do what they are not supposed to do within its full active sense. Social engineering happens in our day-to-day lives. One can use social engineering within their friend's circle to make things work out in their favour, during street shopping one can use social engineering to bargain the price of a product or as a student, try to convince a teacher after failing to complete his homework on time. In information security, social engineering has a different meaning. In cyber security, social engineering is considered a cyber-attack.

Social engineering is the most used cyber-attack by threat actors in current times. Ransomware groups, Advance persistence teams, scammers, and other threat actors use social engineering before conducting advanced technical attacks. The bigger the target, the more sophisticated the art of deception can get on the cyber playground. The success of cyber-attacks depends upon the social engineering manoeuvre of threat actors. As the internet and its users grow across the world, cyber security firms have also captured massive coverage to spread awareness among common users, government entities, and private organizations about potential cyber-attacks. Though their target could be anyone depending on their interest, for a successful attack, attackers must indirectly fight with cyber security firms who frequently dismantle the latter's tactics and techniques by releasing cyber security updates. With the help of these updates on the internet, users have evolved to intercept common social engineering attacks they face or potentially might face. However, threat actors have not given up on their vicious intention to accomplish their aim. They are frequently creating and inventing new social engineering attacks to exploit unintended loose ends of the human brain. They constantly change their social engineering attacks by leveraging geopolitical events, religious issues, war, social issues, data leaks, pandemics, etc. Social engineering attacks are always there in the arsenal of threat actors to make victims fall into their malicious cyber trap. It is extensively used for pushing the victims to interact with malicious files or malicious uniformed resource locator [URL] and to fetch critical information by engaging with the victim via e-mail, chatting, or phone call. Social engineering attack plays a more important role when threat actors are not technically or resourcefully advanced.

SOCIAL ENGINEERING METHODS

Social engineering is an important attack for threat actors to create a base for actual advance technical attacks. The attacks can be planned into three parts. These methods depend upon the threat actor's long-term and short-term aims, whether their malicious intention could be achieved through one-time information, or they want to keep information flowing throughout the month or a year. Below we discuss various types of social engineering attacks.

STRATEGIC ATTACK

This is a highly sophisticated and complicated attack where the threat actor perfectly maintains a disguised or fake identity to keep engagement active with the victim. The attack is performed with the aim of a long-term goal. They operate as a spy but virtually. If this attack is successful, then it could benefit the threat actor in fetching the required basic information and help the threat actor to drop their malicious content with not many hurdles.

One of the benefits of a Strategic attack is if threat actors fail in the first attempt, then they will come out learning more about the victim such as his/her likes and dislikes which will help the threat actor to craft a second attempt with a more accurate strategy with high chances of a successful attack.

Not all threat actors are advanced, so many attackers rely on social engineering attacks with strategic approaches. It's not always that threat actors can bypass all the technical challenges they face. Sometimes they must pull their social engineering skills to avoid detection by making the victim disable anti-viruses or maybe sometimes threat actors need to make the victim interact with complicated technical tasks to execute the malicious file successfully. Successful Strategic Attacks always make sure the victim is ready to hear the threat actor's commands and follow them.

TACTICAL ATTACK

This attack is based on clickbait and is technically advanced enough to make sure the victim must interact very less with malicious links or files. This attack usually takes leverage of geopolitical events, social issues, religious issues, war, politics, and other issues or contexts which instantly trigger the human mind to react to it. The attack is usually conducted on mass targets with the same social engineering attack. However, with time, approaches may change. In many cases, it is found that threat actors used the same social engineering attack on various targets and then suddenly shifted to a new issue after coming to the notice of cyber security firms. The tactical attack is always aimed at a quick compromise of the victim's device.

LATERAL MOVEMENT ATTACK

This attack follows a "successful breach" into the victim's device. The security community must have read and heard about "threat actors moving laterally". These attacks come under the very same lateral movement attack. During the attacks, the art of social engineering becomes easy. However, they avoid instant attacks on victims connected to the compromised user. They wait and monitor the compromised victim's activity for a few days and in some cases a year or months. After they finish collecting information, they monitor to find out which social media or chatting messenger the compromised victim is NOT using frequently. After the confirmation and burning of the victim's valuables, they conduct lateral movement attacks using the already cooked-up genuine profile of the victim. This way, threat actors don't have to put extra effort into perfect deception mode, providing an extra edge for social engineering attacks to drop malicious links or files.

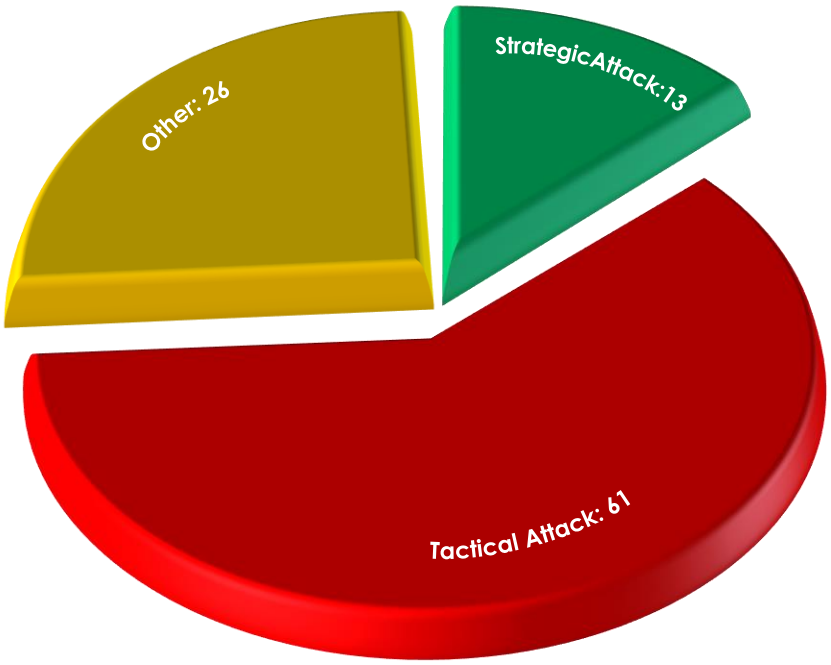
THE PSYCHOLOGY BEHIND SOCIAL ENGINEERING

This is one of the most important aspects of social engineering attacks. After intense reconnaissance and search, the threat actor uses the accumulated data to find the state of mind that the victim is in. The data is used for analyzing the victim's character, nature, behavior & mental status. Accumulated data helps threat actors to know the psychological status of the human mind, it helps them with low-level or medium-level confirmation of the victim's interaction with malicious content. During the initial stage of many attacks using accumulated data, threat actors are somewhat sure of compromising the victim even before they execute a social engineering attack.

In many cases, actors have even compromised the victim who was already alerted to being targeted. They pushed victims to interact with malicious content - a specially crafted social engineering attack - to make the victim feel that the malicious channel is safe to use for online communication. However, the application was wrapped up with malware. Threat actors found loose ends in human minds and successfully exploited the state of alertness (or lack thereof) of the victim. This is only possible when threat actors know about the victim's state of mind.

STATISTICS

CYFIRMA research team reviewed 100 cyber-attacks by various prominent threat actors to detect the type of social engineering attack. Statistics indicate that out of 100 attacks in the last 18 months, 13 attacks were using strategic social engineering attacks and 61 were tactical attacks, the remaining 26 were under other attacks such as web attacks. Listed below are some notable examples.



UBER ATTACK

In one of the recently reported attacks by various media outlets and security firms, a hacker used a tactical social engineering attack to get an MFA approved by Uber's employees. The hacker had stolen log files purchased from the dark web market that contained the credentials of two employees who were working at Uber. The log file contained credentials of Google, Facebook, Twitter, Uber, Instagram, slack, and many more internet platforms. The hacker logged in to one of Uber's internal sub-domains, then kept on sending a push notification, hoping to get approval on MFA. However, when it didn't work, the hacker impersonated the IT guy and convinced the victim to approve. After the fact, the hacker opened doors for random users to communicate with him, and he shared his experience and process that he chose to compromise Uber. However, a bunch of information must have given him the confidence of pulling this menace with a pinch of social engineering attack to take this cyber-attack to a whole new level.

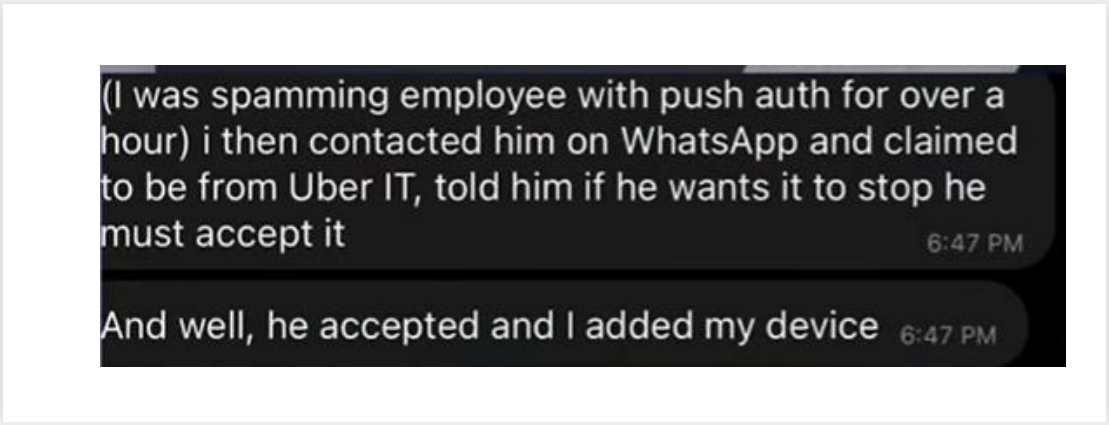


Figure 1 Hacker tells how he convinced the victim to approve MFA.

He triggered the victim's mind with an unexpected request which could only be possible if the Uber IT team would have reached him in real. The victim had no idea of his credentials leaking to a third person and the attacker knew it. So, the threat actor moved tactically and didn't give enough time for Uber employees to think and consider it could be social engineering, the signature of a cyber-attack.

ATTACK BY KIMSUKY

Kimsuky is an advanced persistent threat group based in North Korea. They are known for launching attacks on the South Korean government and UN officials. In the month of August Kimsuky launched a spear phishing campaign backed by a strategic social engineering attack. The threat actor impersonated a Korean government official and requested consultation on the report related to the "Situation in Korean Peninsula". When the victim agrees to follow up on the consultation request then the threat actor reverts to email with a malicious file. If the victim denies the request, then the threat actor replies with no attachments, which also, hints at attempting the attack again at a later date.

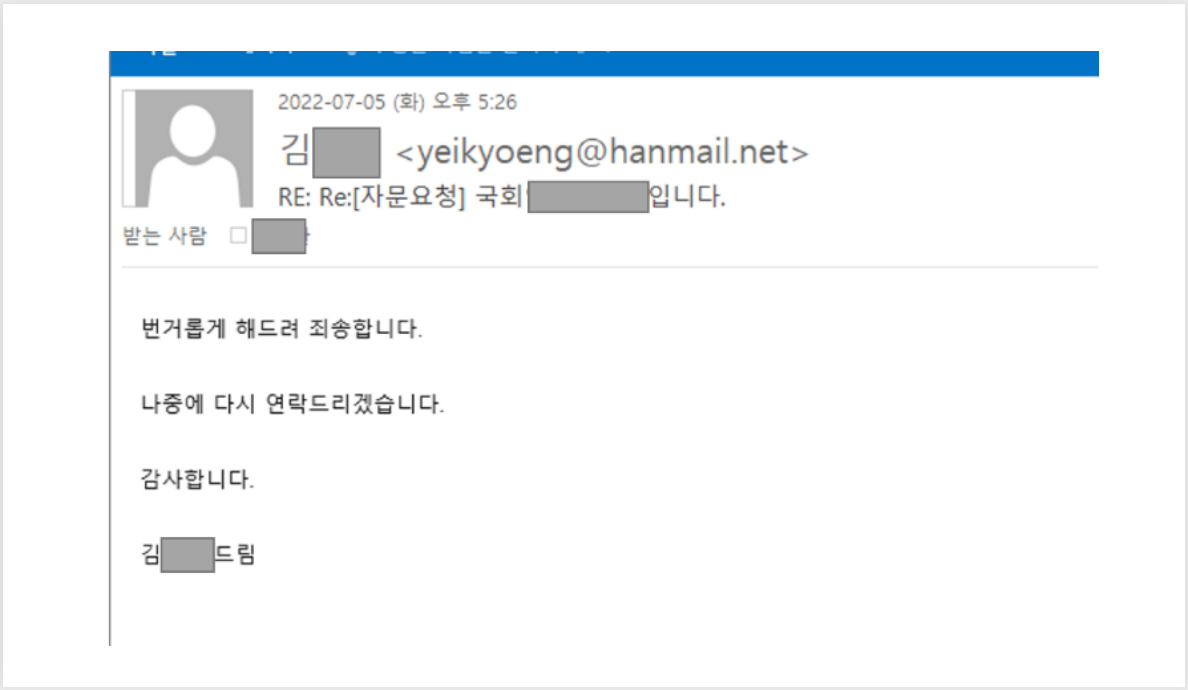


Figure 2 When Victim declined to comply with the request

Translation: We will make it a hassle and we will bless you."
We will get back to you later.
I appreciate it.

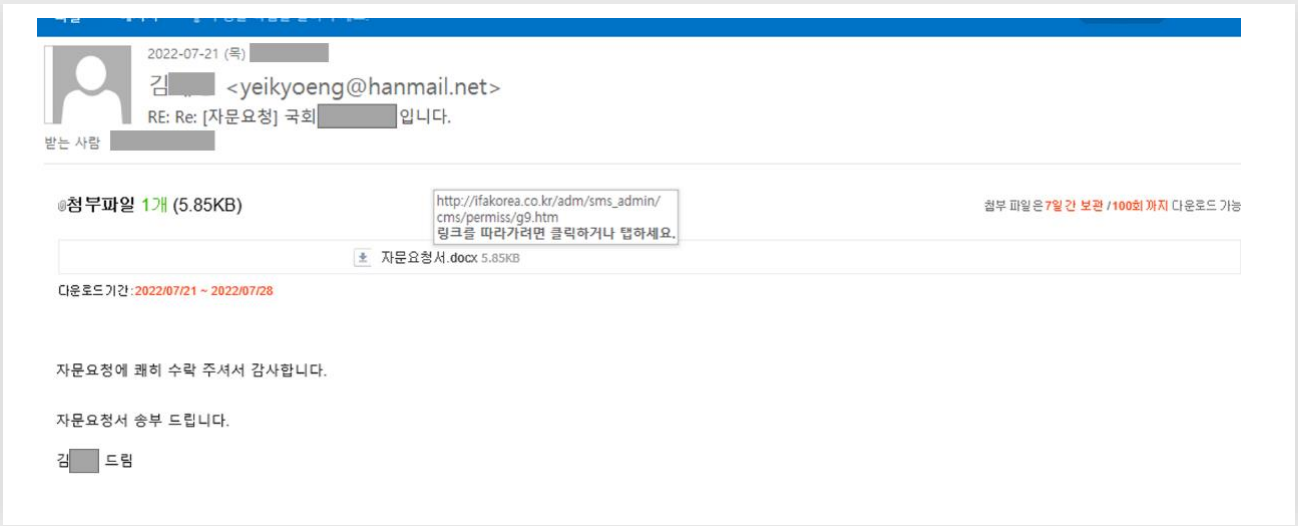


Figure 3 When the victim accepted the request to go through the report.

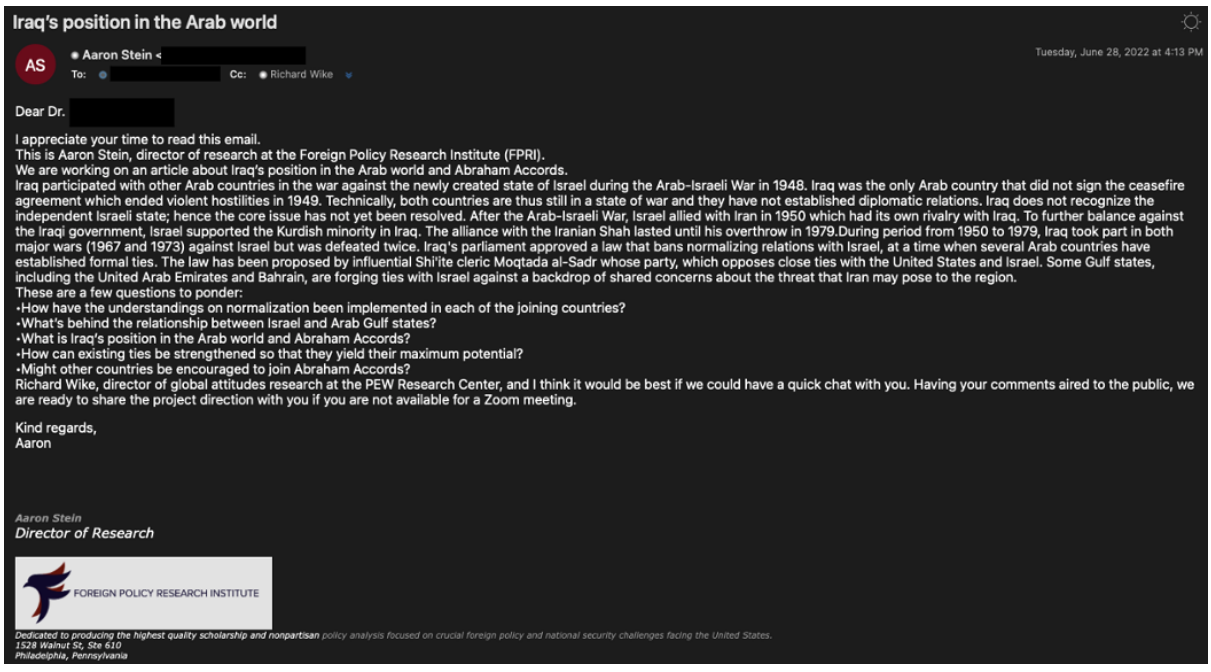
Translation: Thank you for your over-acceptance of the Advisory,
Advisory Letter Transmission Drip LI

This unique social engineering attack gives a sort of confirmation to the threat actor about whether the potential victim is going to interact with a malicious file or not. Such a social engineering approach will also limit the spread of

malware which will reduce the chances of the malicious file being detected or coming under the radar of an anti-virus company.

ATTACK BY TA453

CYFIRMA noticed another unique social engineering play by Iranian APT TA453 who understood the utility of social engineering attacks in the well-planned cyber-attack. In fresh attacks, TA453 implemented a strategic social engineering attack against the target with the profession of medical research. More than one disguised identity as officials from foreign policy research institutions was created and added to be part of a group discussion via email. They sent a well-crafted email discussing the relationship between Iran and Israel. This was a strategic attack, so, dropping off malicious links straight to the victim wasn't the plan, they intended to keep the victim engaged in conversation and leverage the context to drop credential harvesting links. The threat actor replied within the same group via another disguised identity to make the victim understand the gravity of the topic and how important it is to them.



Iraq's position in the Arab world

AS ● Aaron Stein <[redacted]>
To: ● [redacted] Cc: ● Richard Wike

Tuesday, June 28, 2022 at 4:13 PM

Dear Dr. [redacted]

I appreciate your time to read this email.
This is Aaron Stein, director of research at the Foreign Policy Research Institute (FPRI).
We are working on an article about Iraq's position in the Arab world and Abraham Accords.
Iraq participated with other Arab countries in the war against the newly created state of Israel during the Arab-Israeli War in 1948. Iraq was the only Arab country that did not sign the ceasefire agreement which ended violent hostilities in 1949. Technically, both countries are thus still in a state of war and they have not established diplomatic relations. Iraq does not recognize the independent Israeli state; hence the core issue has not yet been resolved. After the Arab-Israeli War, Israel allied with Iran in 1950 which had its own rivalry with Iraq. To further balance against the Iraqi government, Israel supported the Kurdish minority in Iraq. The alliance with the Iranian Shah lasted until his overthrow in 1979.During period from 1950 to 1979, Iraq took part in both major wars (1967 and 1973) against Israel but was defeated twice. Iraq's parliament approved a law that bans normalizing relations with Israel, at a time when several Arab countries have established formal ties. The law has been proposed by influential Shi'ite cleric Moqtada al-Sadr whose party, which opposes close ties with the United States and Israel. Some Gulf states, including the United Arab Emirates and Bahrain, are forging ties with Israel against a backdrop of shared concerns about the threat that Iran may pose to the region.
These are a few questions to ponder:
•How have the understandings on normalization been implemented in each of the joining countries?
•What's behind the relationship between Israel and Arab Gulf states?
•What is Iraq's position in the Arab world and Abraham Accords?
•How can existing ties be strengthened so that they yield their maximum potential?
•Might other countries be encouraged to join Abraham Accords?
Richard Wike, director of global attitudes research at the PEW Research Center, and I think it would be best if we could have a quick chat with you. Having your comments aired to the public, we are ready to share the project direction with you if you are not available for a Zoom meeting.

Kind regards,
Aaron

Aaron Stein
Director of Research

FOREIGN POLICY RESEARCH INSTITUTE

Dedicated to producing the highest quality scholarship and nonpartisan policy analysis focused on crucial foreign policy and national security challenges facing the United States.
1528 Walnut St, Ste 610
Philadelphia, Pennsylvania

Figure 4 TAs disguised identity part of SE attack

Figure 5 Persona 2 replied to the same email expressing his expectation of a reply

This attack had lots of resources put on the job. Considering the effort and resources it reflects that the target was a high-profile individual. The threat actor created an environment to control the whole conversation and psychologically tried to make the victim feel that his views are very important and that he should express his thoughts via responding to the emails. Even though the topic chosen against the victim was medical research, the background didn't have convincing power. Choosing a topic related to medical research could have backfired as one must have an equal level of knowledge to keep conversational engagement active. So, the threat actor tried to leverage the always contentious geopolitical and diplomatic relations to bring victims to the point where they could share links or files.

SOCIAL ENGINEERING DEPENDENCY ON ADVANCED TECHNICAL ATTACK

In some events, threat actors finalize social engineering attacks by first considering advanced technical attacks. They plan social engineering attacks on the basis of advanced technical attack options available to them. Assume a scenario where threat actors have access to "open redirection" vulnerability in a reputed media house's website. The victim is a high-profile individual from a government entity or a reputed multibillion/million-dollar company. Then threat actors could decide to take a disguised identity of a journalist and through social engineering attack, they can deliver the malicious file or link using open redirection vulnerability. Displayed below is a captured HTTP request as a proof of concept from the Break the security vulnerability-lab reproducing an open redirection bug that points to a malicious link.

```
GET /btslab-master/vulnerability/url/open.php?u=http://www.malicious-link.com HTTP/1.1
Host: localhost
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36

HTTP/1.1 302 Found
Connection: Keep-Alive
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Date: Thu, 08 Sep 2022 04:59:53 GMT
Keep-Alive: timeout=5, max=100
Location: http://www.malicious-link.com
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29
X-Powered-By: PHP/7.4.29
```

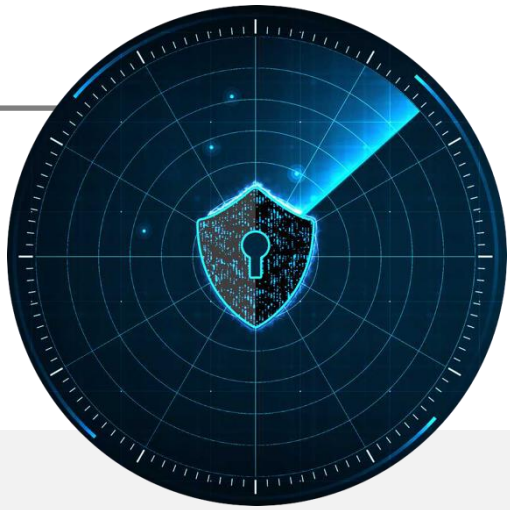
Figure 6 Live Http captured request while reproducing OR vulnerability.

In the past, Microsoft has warned its readers about open redirection vulnerabilities being abused for delivering malicious files and redirecting users to phishing pages. Big firms like Facebook, Google, and Microsoft reward well for finding the OR vulnerability in their web applications. In recent attacks, OR

vulnerability in American Express was abused by threat actors to deliver the phishing page.

Open redirection is a highly destructive vulnerability when it comes to delivering a malicious file or link.

DETECTION



Detection of social engineering attacks can reduce the number of successful cyber-attacks in its initial stage. Following are a few points that we can keep in mind to dismantle any cyber-attack in the future:

1. Always be alert when any unknown user tries to reach different communications points. Also, verify if the unknown user has taken the name of a person known to you as a reference to start the conversation.

2. Be very sure before trusting any mail or message that arrived related to any ongoing issue like the pandemic.

3. Analyze on your own the number of important files you carry being an internet user and what pieces of information have the potential to attract a cyber thief. Stay alert according to the outcome of this analysis.

4. Conduct regular VAPT sessions to get rid of vulnerabilities like OR that could be leveraged by threat actors to deliver malware or infect users or employees.

5. Always confirm before clicking on the file that was shared by connections on social media or emails received from contacts after a long-time gap.

6. Cross-check before engaging further with the user who is prompting, again and again, to click or visit any link.

7. Always be alert when the user asks to open any link or file through a WhatsApp call. Chances are high that the received WhatsApp calls could be from a virtual number, as threat actors always avoid using any real SIM.

8. Always cross-check via call or any other mode of reliable communication before opening any file that is shared by employees such as IT personnel or HR.

EXTERNAL THREAT LANDSCAPE MANAGEMENT ATTRIBUTION

In the past, wars used to be fought with bombs and missiles. However, with the advancement of technology and rapid digitalization, most wars are now being launched in the cyberspace. For instance, the ongoing Russia-Ukraine escalation witnessed a destructive cyber-attack preceding the actual real-world attack by Russian ground forces. The Ukrainian cyber assets too were deployed to geolocate the Russian defense personnel posted on the war field. Ukrainian cyber attackers used social engineering tactics as the first base of their attack, so as to facilitate targeted missile attacks on the Russians. Human error has always been highlighted as the weakest link in the security chain of any organization – it is this link which the evolved TTPs of social engineering uses to launch massive offensives in the war front.

Cyber-attacks have effectively evolved into warfare, war crimes, bank robbery, personal damage to an individual, and are bringing successful ventures to dust. Many real-world crimes are now replaced with equally destructive and far-reaching cyber-attacks, with social engineering serving as the instigator of these attacks.

With increasing complexity and guile, the modern-day social engineering attacks are leaving the cyber security community in shock that attackers can go to any extent to compromise victims. The recent Uber attack is one of the big examples – of attackers going to great lengths to fool potential victims. As the threat of cyber-attack is increasing day by day, even social engineering attacks will take different shapes which depends upon the creative mind of the attacker and their ability to escalate events to ensure maximum damage. Herein, the detection of this attack has the potential to dismantle cyber-attacks in their initial stage if rightly followed up.

CONCLUSION

Social engineering attacks are the base of the most advanced cyber-attacks, which are tough to avoid for anyone who has open communication lines such as email, messenger, social media, and many more. The threat actors are always trying to stay ahead of cyber defenders, cyber security firms and are always dodging defensive walls created by awareness on latest social engineering tactics used. In most cases, it is always the human presence of mind that can prevent the first stage of a cyber-attack. And likewise, in most cases it is due to human negligence that threat actors can perform successful social engineering attacks. Following up on the detections mentioned here-in could stop many cyber-attacks.

CYFIRMA
DECODING THREATS

CYFIRMA is an external threat landscape management platform company. We combine cyber intelligence with attack surface discovery and digital risk protection to deliver early warning, personalized, contextual, outside-in, and multi-layered insights. Our cloud-based AI and ML-powered analytics platform provide the hacker's view with deep insights into the external cyber landscape, helping clients prepare for impending attacks. CYFIRMA is headquartered in Singapore with offices across APAC, US, and EMEA. The company is funded by Goldman Sachs, Zodius Capital, and Z3 Partners.