A · P · U

ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Security Operation Center and Incident Response Individual Assignment

Thomas MacKinnon TP066728
Intake Code: APDMF2204CYS(PR)
Module Code: CT111-3-M-SOC
Dr. Julia Binti Juremi
Date Assigned: 14/06/2022
Date Completed: 15/08/2022
Word Count: 1882

Contents

List of Figures

1 Introduction

The Federal Bureau of Investigation's (FBI) Internet Crime Report stated that Phishing was the most popular attack used by Cyber criminals throughout 2020, as seen in Figure 1. Phishing is a form of Social Engineering attacks, which focus on exploiting people through manipulation and lies. This is often seen through fraudulent emails, claiming to require victims to urgently submit sensitive information to save their account. The victim will often be prompted to login on a fake website, which is often indistinguishable from the real one (Berasategui, N.D.). The harvested login details can then serve as an entry point to an otherwise impenetrable network. However, other sensitive information could also be the aim of the scam, such as banking details to be used fraudulently.

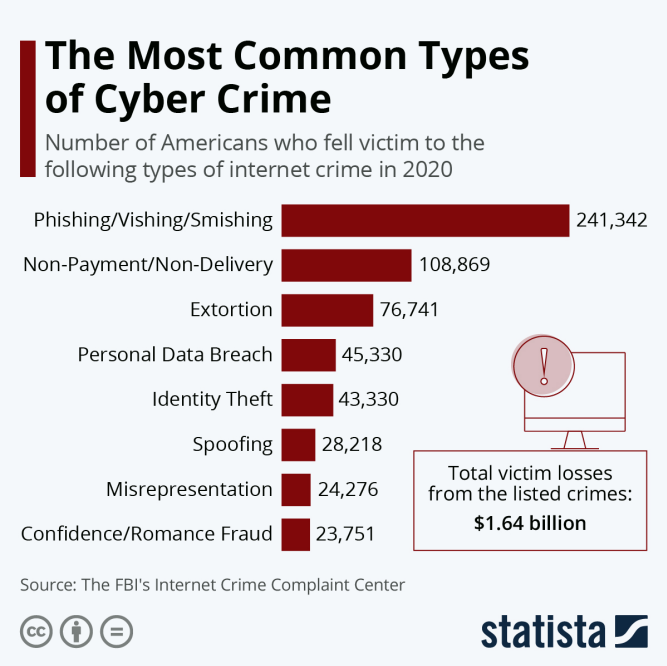

Figure 1: Graph showing Social Engineering to be the most common attack types in Cyber Crime in America throughout 2020 (Ritcher, 2021)

Large companies and organisations are often the target of phishing attacks, with numerous reasons to why the malicious hacker is targeting them. Spear Phishing is often conducted against important figures, like CEOs, where personalised phishing attacks are released against a specific target in order to compromise them or the network (Trend Micro, N.D.). CEOs often have unrestricted access to a companies network, and have little technical or security knowledge to spot a Phishing attack before it is too late.

It is the job of the Security Operation Centre and the associated team to spot these dangerous Phishing attacks and stop them before it is too late. A SOC team is also responsible for preventing such attacks from occurring in the future, but how does a Phishing Attack show up for an SOC team? What does the alert look like? and what evidence is left behind after an attack?

This report aims to answer these questions, by conducting thorough research into the topic of Phishing, followed by a simulated attack on a consenting email address. The attack will be analysed through and all evidence recovered from the attack. This experiment will be used to build an Incident Response Plan for future attacks, with the goal of better upgrading and protecting the network.

2 What is Phishing

Phishing is the "art and science of skillfully maneuvering human beings to take action in some aspect of their lives that may or may not be in the target's best interest" (Lekati, 2018). Phishing is seen through the use of spam emails, as seen in Figure 2, urging the user to click a malicious link that leads to further exploitation. Phishing scams rely on the target believing that it is from a legitimate source rather than some Malicious hacker. It can often be used to harvest sensitive information, but also as an entry point into a secure server.

Phishing employs the use of fake websites that look identical to the real deal, often with a form to submit sensitive information like login details or banking information. The Public are numb to the idea of submitting these details online now, as many services ask for sensitive information before a product can be purchased or a website can be accessed (Dhage & Patil,2019). Phishing effectively exploits this to harvest data that victims would not normally give up.

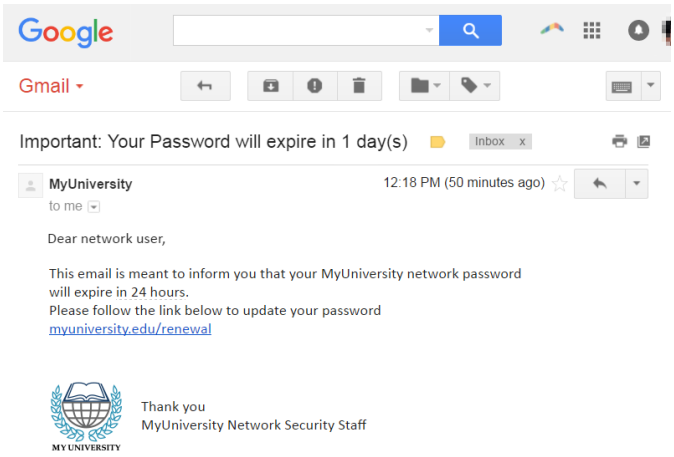

Figure 2:

Almost all phishing emails contain a malicious link, disguised at a https request, which will redirect to the HTTP address to avoid user suspicion (Higashino et al. 2019). There are many techniques out there to make a phishing scam look more legitimate, which further aid in tricking victims.

3 Performing a Phishing Attack

Phishing attacks are surprisingly easy to perform, as this section of the paper proves. Toolkits dedicated to phishing attacks have become rather prevalent, with many free options available through GitHub, or paid options that tend to be better equipped to exploit victims (usually with an address book full of emails to send to included). For this experiment a free option will be tried against a consenting email address, being the Researchers University email, and the results will be captured. The more expensive options are out of scope for this paper, and it is unethical to support Cybercrime as a Service (CaaS) businesses.

The phishing toolkit selected was Blackeye (GitHub, 2018), which was installed using the commands seen in Figure 3, and the shell file was made executable by using `chmod +x blackeye.sh`.

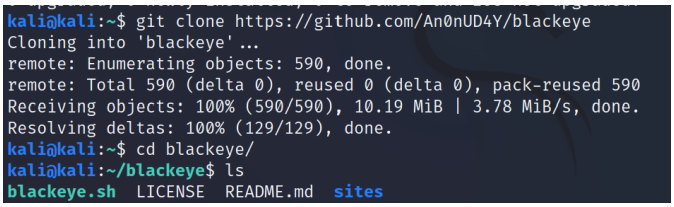

Figure 3: Installing Blackeye Phishing toolkit

Blackeye does the hardest part of the phishing process for the user, by having ready to go fake login pages that look identical to the real ones. The program can be run with the command `sudo ./blackeye.sh`, which produces the selection screen seen in Figure 4, allowing the user to choose any of the thirty two login forms to make a phishing link around.

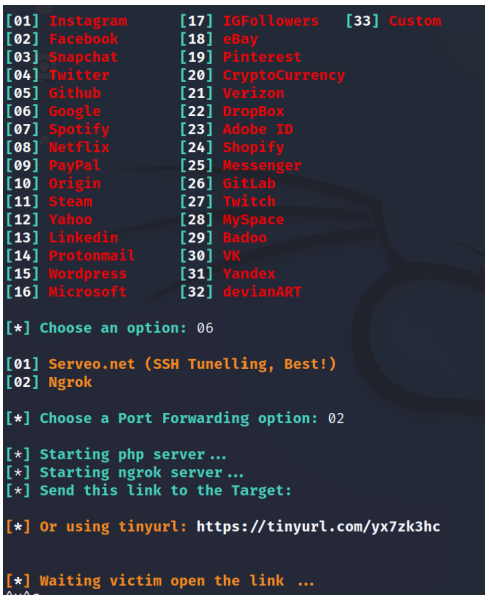

Figure 4: Blackeye start screen, showing options for attack and produced Phishing link

The Blackeye project is four years old at this point, so it needs a little maintenance to get running, mainly by setting up a tunnel to retrieve user information from. NGROK is the tunnel service of choice for this experiment, which requires a user to set up an account before the phishing attack could be performed. Once an account has been created (and verified) an authentication token will be generated which needs to be added to the blackeye directory using the following command, replacing "TOKEN" with the real token.

```
./ngrok authtoken TOKEN
```

This would allow BlackEye to work in the past, however, NGROK has cracked down on people using its services to send phishing attacks, so a work around has to be done, otherwise no phishing link will be produced. In the Blackeye terminal type `./ngrok http 8080` to manually start NGROK, then in a second terminal change directory to the attack site of choice, in this case it would be Instagram, so `cd /blackeye/sites/instagram`. Now setup a PHP client using the command `php -S localhost:8080`, which will produce a link similar to the one seen in Figure 5 in the original terminal.

Figure 5: NGROK manually started to produce a phishing link

4 Evidence of the Attack

The link produced can be used to harvest credentials in any way, from a simple text message to a fully designed email in order to properly exploit a victim. The link is also obviously suspicious, so it can be disguised through several redirects to avoid losing victims. For the sake of this experiment a simple email with the raw link was sent, since the target of this attack was the author. The received email can be seen in Figure 6.

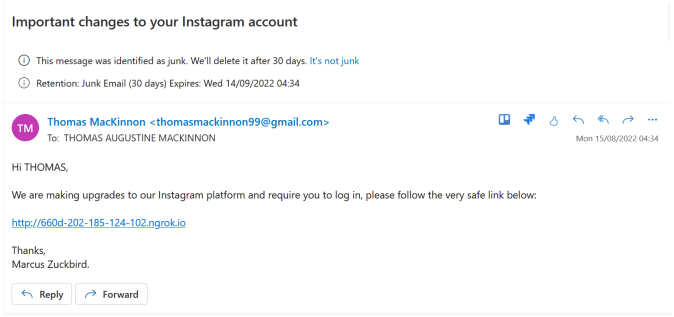

Figure 6: Received email on victim mailbox

The link directs to the site seen in Figure 7, which is a pretty convincing fake Instagram login form, and will notify the NGROK client seen in Figure 5. However, the lack of updates on the project means that no images show up during testing, which makes the page a lot more suspicious to potential targets.

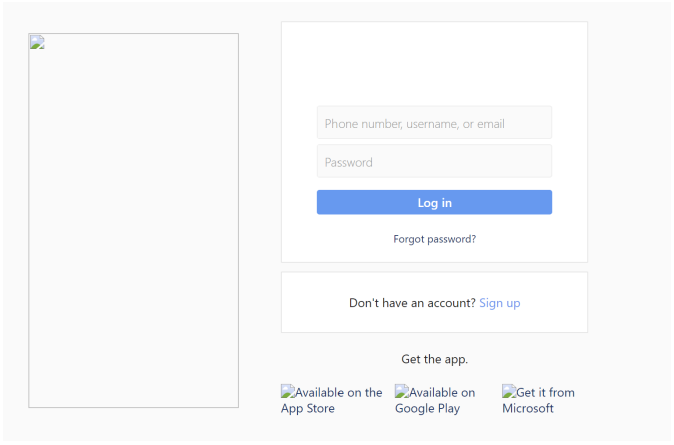

Figure 7: Fake Instagram site login

Furthermore, when submitting login information through the fake Instagram form only an error message was achieved, followed by the shutdown of the NGROK client. This is due to NGROK cracking down on people using their service for phishing attacks, and have since made it against their Terms and Conditions to do so. The associated NGROK account was banned the minute

that the login information was sent through, closing the tunnel off and preventing future use on that account. Additionally the ban appears to be IP based, as trying to create new accounts did not work. This is inconvenient for this experiment, however, very honorable from NGROK, as it prevents future victims from being created from this easy to perform scam.

Google Chrome and Firefox both put several warnings before allowing access to the site, warning the user that it is malicious and having the user agree to enter at their own risk. The site was also clearly not running HTTPS which was made apparent by both browsers. The email was sent directly to the SPAM folder and had warnings when clicking the link. This is all positive developments in stopping users from giving up their sensitive information to phishing scams.

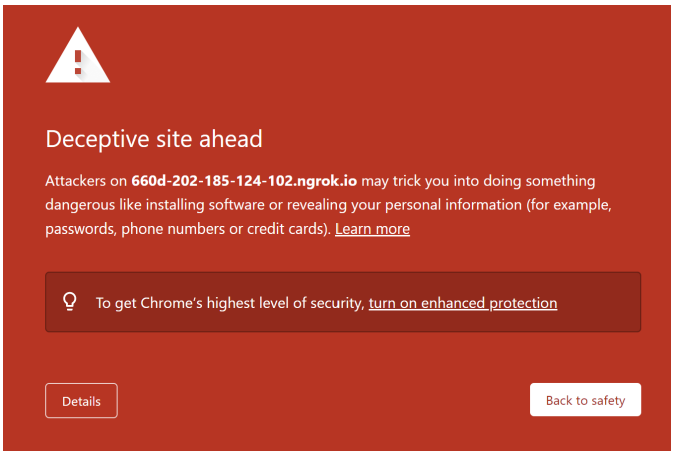

Figure 8: Chrome warning the user of a Phishing site

5 Incident Response Plan

As phishing is the biggest Cyber attack facing businesses today a proper Incident Response plan should be put in place, so that Phishing attacks are handled correctly without any important steps being missed out. An Incident response plan has been developed to mitigate the effect of a Phishing attack, using trusted sources like the Scottish Government's Cyber playbook (Cyber Resilience Unit, 2020).

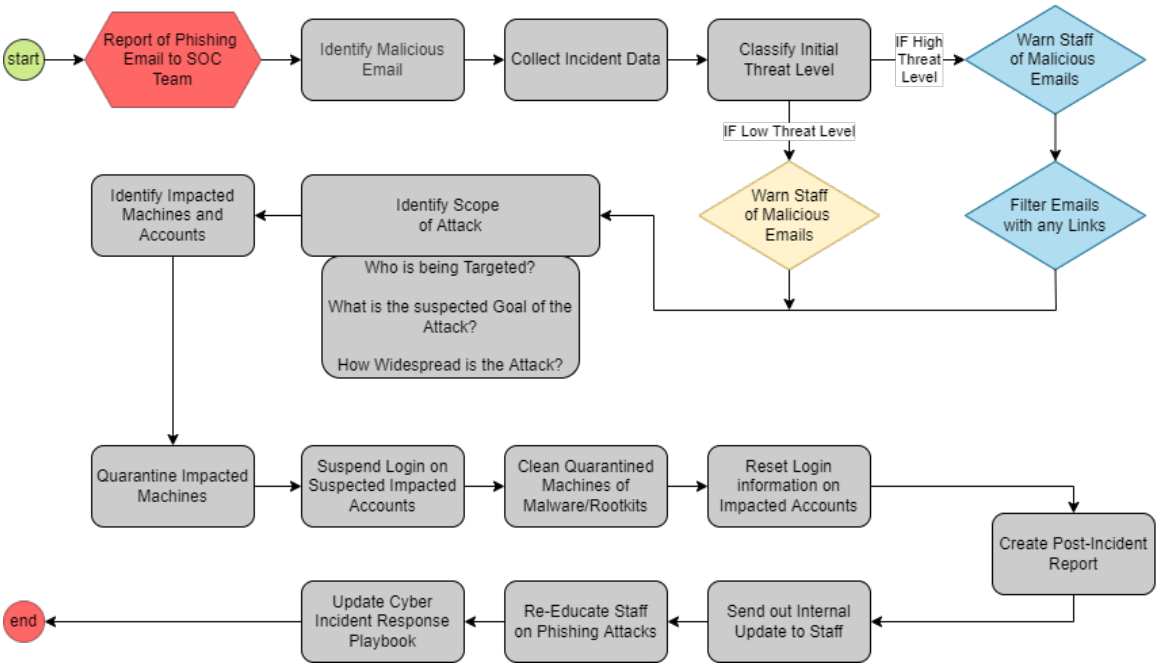

Figure 9: Cyber Playbook for dealing with Phishing attacks

The Cyber Playbook has been illustrated in the form of a flowchart, as seen in Figure 9, but has also been describe in detail so as to avoid confusion.

- **Identify Malicious Email -** Find the first reported email, marking it as patient zero.
- **Collect Incident Data -** What was the goal of this Individual email? Was it trying to harvest account details or install malicious software?
- **Classify Initial Threat level -** Depending on the severity of the attack the initial Class level should be decided. Staff should be warned about the attack regardless of the threat level and informed on what to look out for. If the attack is seriously damaging then the Email filter should be upped to block all links in emails as a precaution.
- **Identify Scope of Attack -** Now that the initial damage control has been done the full scope of the attack can be analysed. Who was the attack targeting (basic employees or is it a spear phishing campaign)? What are the attackers aiming to get out of the Phishing emails (login details, banking information, malware into the system)? How widespread is the attack? These questions help build up a proper threat level for the phishing attack.

- **Identify impacted Machines and Accounts -** Find all possible accounts or machines that the phishing attack could have affected.
- **Quarantine all Impacted Machines -** Any potential device infected from malware from the phishing attack should be quarantined, with a bias towards false positives as to mitigate the chance of an infected machine slipping through the cracks.
- **Suspend Login on Suspected Impacted Accounts -** Yet again any suspected account should have login deactivated to prevent any Malicious hackers getting into the system.
- **Clean Quarantined Machines of Malware/Rootkits -** Thoroughly remove any malware/-rootkits so the machine can be used again without fear.
- **Reset Login Information on Impact Accounts -** So that any credentials harvested are no longer usable.
- **Create Post-Incident Report -** Detailing all that happened during the incident for future use.
- **Send out Internal update to Staff -** Discussing how the incident is resolved, and how to report future Phishing emails in the future.
- **Re-Educate Staff on Phishing attacks -** Education is one of the best ways to mitigate the risk of a future attack, and very cost effective. Making staff more resilient is key to stopping future Phishing attacks.
- **Update Cyber Incident Response Playbook -** With everything learnt from this incident to better deal with attacks in the future.

6 Conclusion

In Conclusion, Phishing is a great threat towards modern day businesses, with the power to steal many employees or members of the public's sensitive information like login credentials or banking details. Phishing also can be a severe threat to any machine, infecting it with malware that can then be used to further exploit a network. The shocking discovery was how easy it is to perform one of these attacks, requiring very little technical skill.

The creation of the Cyber Playbook for Phishing will help any SOC team mitigate the effects of a successful attack, by systemically removing threats and restoring the network, whilst learning from the process. Phishing attacks are becoming harder to launch with Internet Browser detection alerting users before accessing dodgy websites and services like NGROK banning any criminals attempting to use their platform. However, it is still important for SOC teams to be ready to combat this popular attack method as to avoid compromising the network, employees, and even themselves.

7 References

Berasategui, G. N.D. Cybercrime: Which ones are the most common threats today? [online] Red Points. Available at:
https://www.redpoints.com/blog/cybercrime/ [Accessed 10/08/2022]

Cyber Resilience Unit, Scottish Government. 2020. Phishing Playbook v2.3. *Cyber Incident Response*. pp 1-23.

Dhage, S. & Patil, S. 2019. A Methodical Overview on Phishing Detection along with an Organized Way to Construct an Anti-Phishing Framework. *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. pp. 588-593.

Higashino, M., Kawamura, T., Kawato, T., Ohmori, M. 2019. An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Information Leakage. *2019 5th International Conference on Information Management (ICIM)*. pp. 82-86.

Lekati, C. 2018. Complexities in Investigation Cases of Social Engineering. *2018 11th International Conference on IT Security Incident Management IT Forensics*. pp. 107-110.

Ritcher, F. 2021. The Most Common Types of Cyber Crime. [online] Statista. Available at:
https://www.statista.com/chart/24593/most-common-types-of-cyber-crime/ [Accessed 10/08/2022]

Trend Micro. N.D. Spear Phishing. [online] Trend Micro. Available at:
https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing [Accessed 10/08/2022]