P.A

OPERATION CHIMERA

PHISHING ANALYSIS MODULE // SECURITY BLUE TEAM

CONTENTS

This information has been gathered from public sources and combined with my own knowledge and experiences for the purpose of Operation Chimera, an online, live blue-team training operation conducted by myself under the alias Known Divide, for the SecurityBlueTeam community.
Follow me on Twitter please!
https://twitter.com/knowndivide

Useful Links:
[1]https://www.sans.org/security-awareness-training/resources/stop-phish
[2]https://www.kaspersky.co.uk/resource-center/definitions/spear-phishing
[3]https://www.phishing.org/phishing-examples

Sources:

[1] https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html

If you've enjoyed this event, please consider donating whatever you can spare to buy me pizza, coffee, and help fund future events! (even £5/$5 will make a huge difference, and it only takes a few seconds).

PayPal.Me
https://paypal.me/KDMentoring

Donating £10 or more will earn you SBT VIP status for 30 days!
https://securityblue.team/get-vip/

OPERATION CHIMERA – PHISHING ANALYSIS

This document is not 100% finished and will be updated within the next 24 hours. Thank you for your patience.

This module is designed to give a look into the world of Phishing Analysis. It is aimed at individuals who are moving in to Cyber, so the material is aimed at an entry-level student. We strongly encourage further reading using the provided sources and any that you find yourself. Want to talk to other hackers about this specific module? Join the discussion in the "phishing-module" channel in the SBT Discord server. There is also a Chimera mega-thread on Reddit. Please make use of this to ask questions and talk to other participants!

WHAT IS PHISHING ANALYSIS?

Phishing is a social-engineering technique, where an attacker sends an electronic message (usually an email) which is disguised to look legitimate, with the intention to retrieve sensitive information such as usernames and passwords or spread malware.

Phishing Analysis is the act of retrieving useful information from malicious emails, that can be used to take defensive measures, and generate phishing metrics which can be used for trend analysis and Threat Intelligence.

WHY IS PHISHING SO IMPORTANT?

Let's start with some powerful 2019 statistics [1] to show you exactly how important phishing is:

- The average financial cost of a data breach is $3.86m (IBM)
- Phishing accounts for 90% of data breaches
- Phishing attempts have grown 65% in the last year

Yeah, it's bad. Phishing is the leading way to breach a company. It's cheap, it's easy, and 'hooking' even one employee could be enough to compromise the security of the user, system, and network.

TYPES OF PHISHING EMAILS

There are a number of different forms of this social engineering technique, however this module will focus on common email phishing techniques. If you're interested in the other types, then do your own searches for Vishing (*Phone Calls*), SMishing (*Text Messages*), Whaling (*High-value Targets*), and Spear-Phishing (*Highly Targeted & Refined*).

Credential Harvester

- Disguised email asks the user to click on a link and enter in their account details.
- Uses websites that are designed to look like the real website for that company.
- Any entered details are usually stored in a hidden directory or emailed to the attacker.
- Commonly 'spoofed' companies include DHL, Microsoft Outlook, and Amazon.

Malicious Attachment

- Email asks you to open an attachment.
- This is usually a malicious 1st-stage payload, which once executed will download additional payloads to the system.
- Some attachments just contain a link to a Credential Harvester.
- Macros within Microsoft Office documents are used to download malware to a system once enabled.

Recon

- Emails that contain no body text, or random characters such as "sasdafa".
- These emails are used to determine if the recipient is a legitimate address.
- If the target address is not in use, the attacker will usually receive a "Message was not delivered successfully" email reply.
- This tactic is used to scout out legitimate email addresses associated with a target, for future use in phishing or social-engineering attacks.

False Positive

- This is when a user flags an email as being malicious/spam, when it is in fact a legitimate email.
- This is usually the result of internal emails having poor formatting or asking the user to click on a link.

Spam

- Emails that are not malicious but are unwanted. Also known as junk mail. These are usually newsletters, discount offers, webinars, etc.

PHISHING TACTICS

I've seen some very clever tricks that hackers use when launching phishing campaigns. Below are a few examples of tactics you may see when working on sophisticated attacks:

- **Typosquatting**: This is when an attacker registers a domain that is extremely similar to that of their target. For example, if the target was WoodworksInc.com, an attacker might register Woodworks1nc*.com*. Notice the '1'(one) instead of an 'I'. At a glance, these look identical. So, if the attacker was sending an email that was supposed to look internal, with a link such as https://www.woodworks1nc.com/payment-update, users may be more likely to fall for it, click the link, and enter their credentials/details in. The above is an example of a Look-alike Typosquat.

- **Using free email services:** By utilizing services such as Gmail and Outlook, attackers are able to send malicious emails to their target for free, and continuously. Although the email addresses can be blocked by the target, it is extremely likely that they will not block based on domain, as @gmail.com, @outlook.com, and @hotmail.com are all used legitimately, and blocking these would have a negative impact to email communications. Luckily these service providers are good at spotting spammers, and shut down their mailboxes pretty quickly.

- **Using multiple sending domains and sending server IPs:** This is by far the most annoying. Usually if one mailbox is sending phishing emails, we can block *mailbox@domain.com*. If multiple mailboxes from one domain are sending emails, we can block **@domain.com*. But when actors start sending from multiple IPs, using free services (Gmail, Outlook – which we can't domain block for obvious reasons), and other domains, it gets a little more time-consuming. At this point we would look at using the subject line(s) as an identifier for denying incoming emails.

P.A

OPERATION CHIMERA

PHISHING ANALYSIS MODULE // SECURITY BLUE TEAM

ANALYZING PHISHING EMAILS

Gathering initial information:

- As soon as we have our hands on a suspected phishing email, we want to gather information about the email and the sender. This will help us in later stages.
- In Outlook save the email as a .msg or .eml file (File > Save As), and open this using your text-editor of choice. From here you should note down information such as the Sender, Sending Server IP, Return-Path, Email Body (these attributes have varying names, such as X-Originating-IP, X-Env-Sender, ReplyTo. You'll become familiar with them all over time, plus some commercial tools can grab all of this for you).

Analyze the malicious content:

- If there is a URL, carefully copy it, and submit it to VirusTotal for analysis and reputation checks. You can view the URL without going to the potentially malicious page using URL2PNG.
- If there is an attachment, you can either detonate it in a Windows virtual machine (turn your network connection off and run Wireshark!) or submit it to VirusTotal or Joe's Sandbox.
- When working in a SOC, you'll have other commercial-grade tools that can help analyze URLs or Attachments and generate reports based on activity.

Inform the recipients:

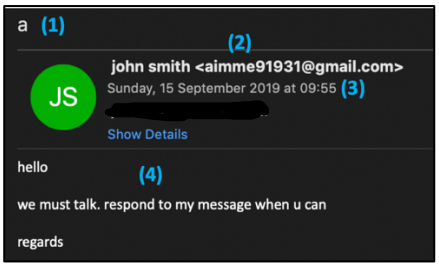
- It's a very good idea to let the recipients of malicious emails know, so that they don't fall victim to them before you're able to take defensive actions such as blocking. A template should be used, and sent to all recipients (in BCC, so they can't see each other's addresses) with the subject line of the malicious email, and a message stating they should not interact with it and delete or report it.

Request defensive actions:

- You need to provide sufficient justification for any blocking actions you want to make, which will be reviewed by peers.
- URLs or malicious domains can be blocked on the web proxy, preventing anyone from connecting to them.
- Attachment file hash values can be blacklisted in antivirus, immediately deleting them if they are discovered within the network.

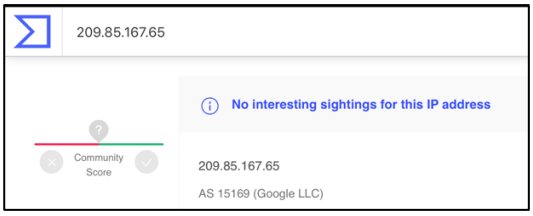
ANALYSIS EXAMPLE ONE (RECON)

- First I'll take a look at the actual email, to see the subject line(1), sender(2), date(3), and body content(4). The recipient will also be shown here, but I've covered it in this example. Because this email is attempting to get a response, and features no links or attachments, it can be classed as Recon.



- Next I'll save the email and open it with a text editor. This will let us look at all of the information contained within the email, that isn't normally visible.

- The first thing that stands out to me is line 9, where it states "spf=pass'. This means that the sender IP is confirmed to be 209.85.167.65 (hasn't been spoofed/faked). As the sender was identified as @gmail.com, this IP must belong to Google LLC. To double-check, I'll put the IP in to www.VirusTotal.com.



- Now let's confirm the Sender, and Recipient, in case they have been spoofed or altered to mislead us. Use CTRL+F to use the Find tool, and search for "To". The following section shows the Sender, Recipient, and Date. The 'Return-Path' is where any email replies will be sent, this can differ from the sending address, as the attacker may use one address to send, and one to receive.

```
From: john smith <aimme91931@gmail.com>
Date: Sun, 15 Sep 2019 09:55:24 +0100
Message-ID: <CAD=3UCF8bcDDy7XZizuhHAzAr2DR8US+JZyjaH1Pu1d2-0HrZg@mail.gmail.com>
Subject: a
To: jordanp23@outlook.com
X-IncomingHeaderCount: 13
Return-Path: aimme91931@gmail.com
```

- Scrolling down within the Text Editor, you will find the email body in both plaintext, and HTML formats. This is a good place to look, as emails may contain a hidden Tracking Pixel, which allows an attacker to see if the recipient has viewed the email. This is usually 1px by 1px, so you won't see it when viewing the email normally.

```
--B_3651386347_1465936617
Content-type: text/html;
    charset="UTF-8"
Content-transfer-encoding: quoted-printable

<html>
<head>
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8">
</head>
<body>
<div dir=3D"ltr">hello
<div><br>
</div>
<div>we must talk. respond to my message when u can</div>
<div><br>
</div>
<div>regards</div>
</div>
</body>
</html>
```

```
--B_3651386347_1465936617
Content-type: text/plain;
    charset="UTF-8"
Content-transfer-encoding: 7bit

hello

we must talk. respond to my message when u can

regards
```

There's nothing hidden in this email, and it appears to be acting solely as a Recon email. As this is very basic, and isn't impersonating a member of staff, there is no real justification to block the email sender yet. However, if a high volume of employees received this email from the same sender, which could suggest signs of large-scale reconnaissance, I would then request *aimme91931@gmail.com* to be blocked on the email gateway, preventing more emails from being successfully delivered.

OPERATION CHIMERA

PHISHING ANALYSIS MODULE // SECURITY BLUE TEAM

MODULE CHALLENGE

If you feel you're familiar with what Phishing is, and how to analyze malicious emails, then you may be ready for the Challenge! We suggest you still do some of your own research using the 'Useful Links' on the first page before attempting the Challenge.

Challenge Brief:
A number of users have reported Phishing emails to the SOC. You need to analyze them to determine the following:

- **Who the real sender is** *(has the sender been spoofed, compromised, or from a free email service?)*
- **The sending server IP** *(where did the email come from)*
- **Any recipients** *(who has received the malicious email)*
- **Analyze any attachments**
- **Analyze any links**
- **Classify the email as Spam, Recon, or Malicious**

After you have retrieved this information, you must fill out a report for each email, stating what actions you believe should be taken, such as blocking IOCs and informing the recipients.

What will I need for this Challenge?

- Microsoft Outlook application
- A throw-away Outlook account
- A text-editor application
- Phishing Module Report Template (Available 16th Sept 8PM)