SIMULATED PHISHING CAMPAIGN REPORT

Conducted By: Tarun Kumar Pathak

Date: 27/12/2024 - 28/12/2024

Institution: Rd Infro Technology

Introduction

Phishing is a kind of cyberattack in which criminals pose as reliable organizations in an attempt to fool consumers into disclosing private information like passwords, usernames, or bank account information. These assaults are frequently carried out using malicious websites, social media, or email. Because of its ease of use and reach, email phishing continues to be one of the most popular and successful techniques employed by cybercriminals.

This report presents the findings from a simulated phishing campaign conducted using the Go Phish framework. The campaign aimed to evaluate the awareness levels and behaviours of the targeted group when faced with phishing emails. The scenario chosen for this campaign was an "Urgent: Change Google Account Password" email.

Types of Phishing:

1. **Email Phishing:**
    - The most common form of phishing, where attackers send deceptive emails designed to lure users into clicking malicious links or downloading harmful attachments.
2. **Spear Phishing:**
    - A targeted form of phishing aimed at specific individuals or organizations, often using personalized information to appear legitimate.
3. **Smishing and Vishing:**
    - Smishing involves phishing through SMS messages, while vishing involves voice calls to deceive victims.

4. **Clone Phishing:**
    - The attacker duplicates a legitimate email and replaces its content with malicious links or attachments.
5. **Whaling:**
    - A sophisticated phishing attack targeting high-profile individuals like executives or decision-makers.

Phishing Campaign Analytics

The campaign was conducted over two days (27/12/2024 - 28/12/2024) and targeted a group of 10 email accounts. Below are the analytics:

Metric	**Count**
Total Email Sent	10
Email Opened	2
Link Clicked	2
Credentials Submitted	2

Scenario:

The phishing email was designed to appear as an urgent notification from Google, requesting users to change their account passwords immediately to secure their accounts. A malicious link redirected users to a fake Google login page where credentials were collected.

Observations:

- 20% of the recipients opened the phishing email.
- 20% clicked on the link embedded within the email.
- 20% submitted their credentials on the phishing landing page.
- The campaign highlights a need for improved awareness and vigilance among the users.

Exporting Campaign Analytics

Using the Go Phish framework, campaign analytics can be exported in formats such as CSV or JSON for detailed analysis. This feature allows cybersecurity professionals to:

1. Evaluate the effectiveness of the campaign.
2. Identify trends and patterns in user behaviour.
3. Present actionable insights to stakeholders.

Creating Groups

For effective campaign management, Go Phish allows the creation of groups based on specific criteria (e.g., departments or user roles). Grouping users helps tailor campaigns to address unique vulnerabilities and ensures targeted training.

Recommendations:

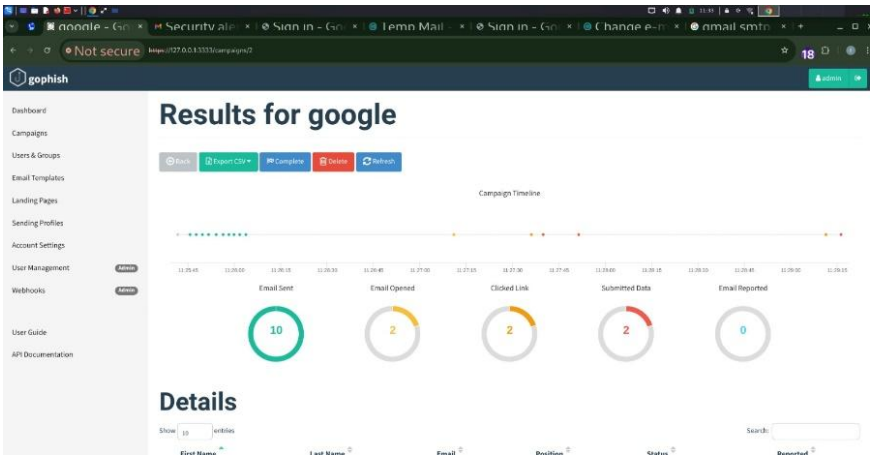
1. Conduct regular phishing awareness training for all users.
2. Share tips on identifying phishing emails, such as:
    - Verifying sender details.
    - Avoiding clicking on unverified links.
    - Checking for grammatical errors or unusual requests.
3. Implement technical measures, such as:
    - Enhanced spam filters.
    - Two-factor authentication.
    - Automated email warnings for suspicious messages.

Conclusion

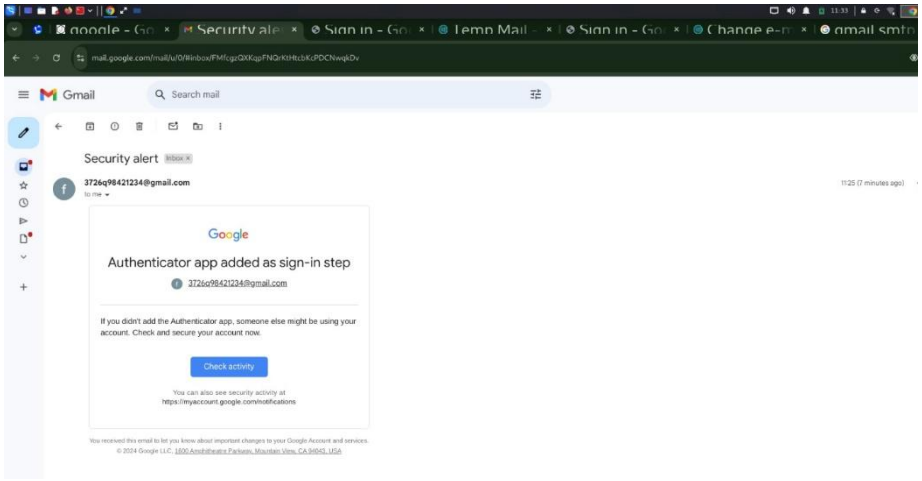
The campaign demonstrated that phishing remains a significant threat, with some users falling prey despite basic security measures. Continuous education and training, combined with robust technical controls, are essential to mitigate the risk of phishing attacks. Future campaigns should aim to reduce the success rate of such attacks by tracking improvements in user behavior.

Attachments

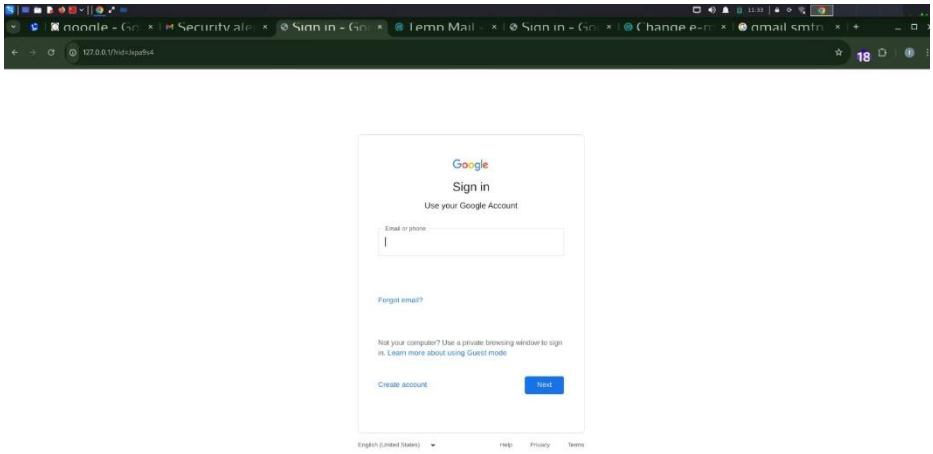
1. **Figure 1:** Screenshot of Campaign Dashboard Summary.



2. **Figure 2:** Screenshot of Phishing Email Template.



3. **Figure 3:** Screenshot of Phishing Landing Page.



4. **Attachment A:** CSV Export Report of Campaign Analytics.

	A	B	C	D	E	F	G	H	I	J	K	L
1	id	status	ip	latitude	longitude	send_date	reported	modified_	email	first_name	last_name	position
2	MzhemZt	Email Sent		0	0	2024-12-2	FALSE	2024-12-2	xyz@gmail	abc	d	
3	mrFlACi	Email Sent		0	0	2024-12-2	FALSE	2024-12-2	aditya.patl	ad	d	
4	Jxpa9s4	Submitted	127.0.0.1	0	0	2024-12-2	FALSE	2024-12-2	3726q984	aditya	kr	
5	jYI4Gi2	Email Sent		0	0	2024-12-2	FALSE	2024-12-2	d@y.com	fd	as	
6	6a1jlAH	Email Sent		0	0	2024-12-2	FALSE	2024-12-2	hapex142	fd	s	
7	L0UMWFf	Submitted	127.0.0.1	0	0	2024-12-2	FALSE	2024-12-2	hapex142	g	gf	
8	WJMtKVx	Email Sent		0	0	2024-12-2	FALSE	2024-12-2	t.kr.pathal	sd	s	
9	4qJubQx	Email Sent		0	0	2024-12-2	FALSE	2024-12-2	kr.pathak.	tarun	kr	
10	OIRVBBt	Email Sent		0	0	2024-12-2	FALSE	2024-12-2	tarun.path	tarun	a	
11	JhPWOR6	Email Sent		0	0	2024-12-2	FALSE	2024-12-2	deathkiller	xyz	kr	