# II. Reconnaissance

## 1. What happened?

The attacker utilised the OSINT framework to gather information of the company from free sources. From the company website, company emails [Mr.s@definatelyarealcompany.com](mailto:Mr.s@definatelyarealcompany.com) and [notascammer@definatelyarealcompany.com](mailto:notascammer@definatelyarealcompany.com) were found. The email domains were scanned using public tools and were found to not have anti-spoofing mechanisms.

A screenshot of a computer

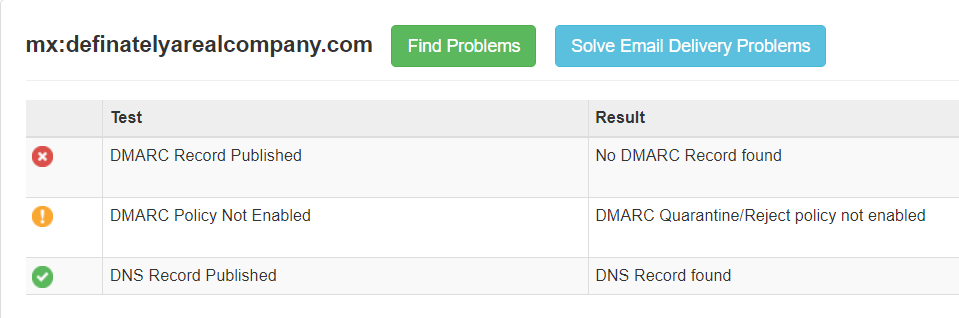
Description automatically generated

Figure 2.1.0.1&2.1.0.2 Mail scan result from <https://mxtoolbox.com> and <https://checkcybersecurity.service.ncsc.gov.uk/email-security-check>.

The attacker then attempted to forge a phishing mail to **Mr. S** pretending to be **notascammer** using Gophish **(appendix 1)**.

A screenshot of a computer

Description automatically generated

Figure 2.1.0.3 Phishing email in Mr. S’s outlook.

A screenshot of a computer code

Description automatically generatedA screenshot of a computer

Description automatically generatedUpon inspecting the mail headers, the group noticed that the mail server was unsecured and did not require authentication on email headers, allowing unauthenticated and malicious emails as such being delivered.

Figure 2.1.0.4&2.1.0.5 phishing mail header and company hmailserver unsecure configuration.

## 2. Email secure protocols SPF, DKIM, DMARC

This part will cover process of securing company email domains for both self-hosted email servers and third-party email services, in this case hmailserver and google workplace.

### 2.1 Sender Policy Framework (SPF)

SPF prevents spoofing by specifying the mail servers allowed to send email using the company domain. SPF publishes a list authorized IP addresses in a DNS TXT record, the server validates the source IP address of email address using the domain based on the list. If email is not sent from an authorized source, it will be marked as spam or will be rejected.

A screenshot of a computer

Description automatically generatedFigure 2.2.1.1SPF graph (Mantra, 2024).

A SPF record usually contains the version of SPF, permitted ip range, SPF list of another domain and what to do when one does not match. Adding SPF to domain requires creating a DNS TXT record on your domain. Since the mail server is hosted at 192.168.1.7, the following SPF record is configured so only this server can send mail from the company domain (definatelyarealcompany.com).

A close-up of a computer code

Description automatically generated

Figure 2.2.1.2 Mail server SPF configuration.

Similarly, google workplace emails uses google SPF record.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Figure 2.2.1.3 Google workplace SPF configuration.

### *2.2* DomainKeys Identified Mail *(DKIM)*

DKIM ensures email integrity and authencity by using a private key as a digtal signature. When there is an email, the server fetches the public key to verify the signature. Emails failed to verify their signature will be quarrentined or rejected.

A diagram of a server

Description automatically generated

Figure 2.2.2.1 DKIM graph (Nicolas, 2024).

A screen shot of a computer

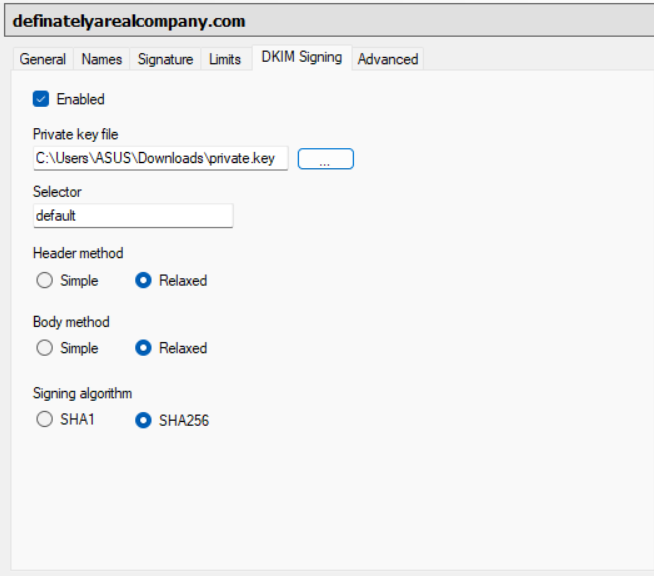
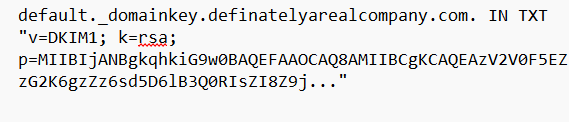
Description automatically generatedA DKIM record usually contains the version of DKIM, encryption algorithm and public key. Adding DKIM to domain requires a pair of public and private key, and creating a DNS TXT record. For local server, a pair of keys can be generated using OpenSSL. The server will hold the private key while the DNS TXT record uses the public key.

Figure 2.2.2.2&2.2.2.3&2.2.2.3 RSA key generation and mail server DKIM configuration.

On google workplace, keys are generated from the admin console and DNS TXT record “google.\_domainkey” must be created. A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

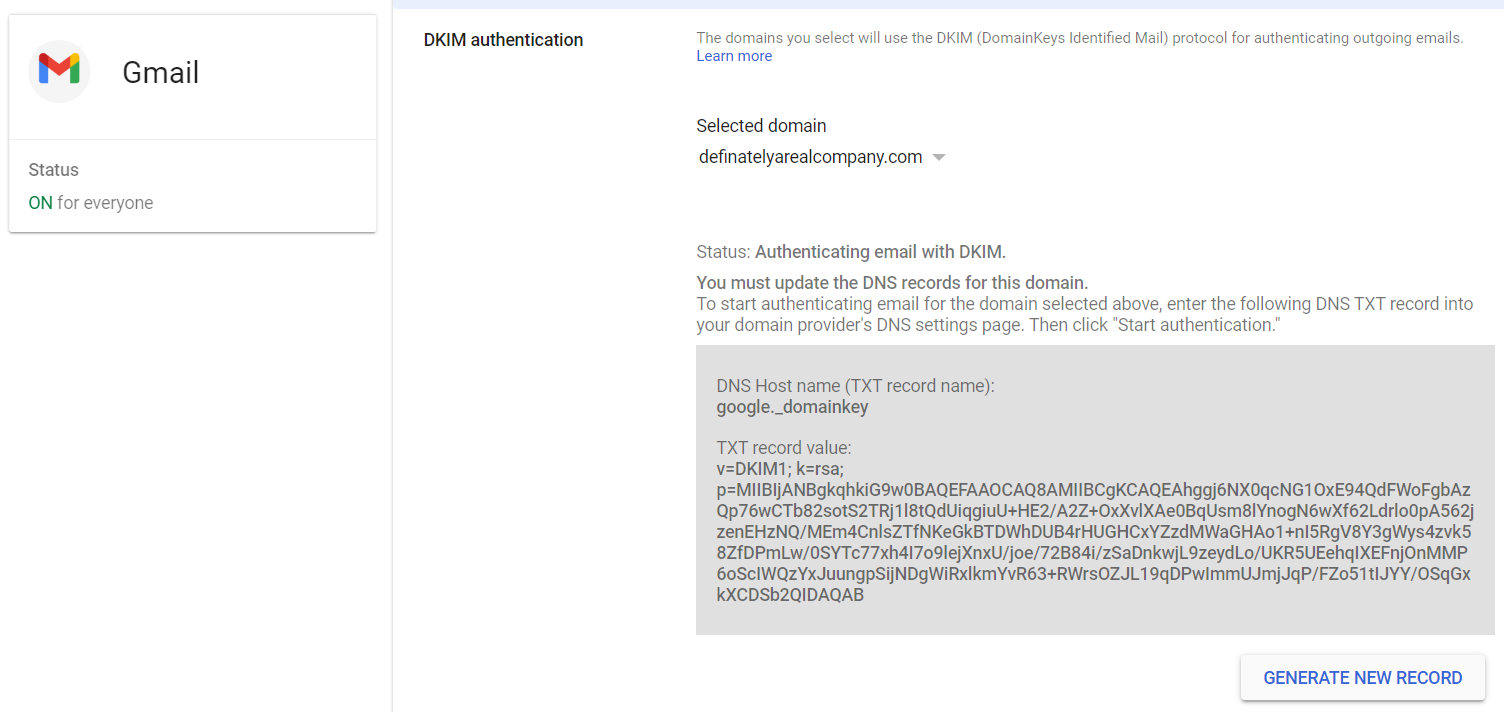


Figure 2.2.2.4&2.2.2.5 Google workplace RSA keys generation and DKIM configuration.

### *2.3* Domain-based Message Authentication, Reporting, and Conformance *(DMARC)*

DMARC provides a unified policy to handles emails that fail SPF or DKIM checks and report them to domain owner. DMARC also ensures the email “FROM” header aligns with the domain in SPF and DKIM checks, providing additional spoofing protection.

A computer screen shot of a computer

Description automatically generated

Figure 2.2.3.6DMARC graph (Mantra, 2024).

A DMARC record usually contains the version of DMARC, policy to handle email failing SPF or DKIM and an email to send report to. Adding DMARC requires a DNS TXT record. 

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Figure 2.2.3.7&2.2.3.8 Google workplace and mail server DMARC configuration.

### 2.4 Testing

A computer screen shot of a computer code

Description automatically generatedA screenshot of a computer

Description automatically generatedNow, the company email domain will be scanned with a test email.

Figure 2.2.4.1&2.2.4.2Email domain scan and email headers.

Since, email security protocols are running, DMARC should trigger if the attacker tries to spoof the email domain.

A screenshot of a email

Description automatically generated

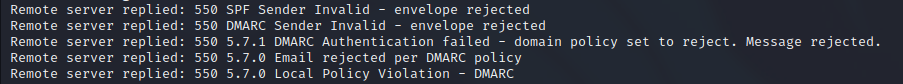


Figure 2.2.4.3&2.2.4.4 DMARC prevents email spoofing.

## 3. Raise awareness against social engineering

To raise awareness against social engineering and spoofing emails, conduct regular training sessions on identifying suspicious emails, implement phishing simulations to test and educate employees. Make a policy requiring employees to verify sender addresses for every email and avoid clicking suspicious links.

## Appendix 1

A screenshot of a computer

Description automatically generated