Hey mate! Sorry for leaving this case with you, had to jump in to an incident response meeting. You can find my notes below, if you can write that report that would be awesome.

I owe you one!

======
Email Artifacts
======

Sending Address:
emailsecalert1@gmail.com

Subject Line:
Your Email Will be Locked! Act NOW!

Recipients:
john.smith@dicksonunited.co.uk
alice.cooper@dicksonunited.co.uk
jacon.long@dicksonunited.co.uk
fred.johnson@dicksonunited.co.uk
pickle.rick@dicksonunited.co.uk

Sending Server IP:
209.85.222.173

Reverse DNS:
mail-qk1-f173.google.com (Gmail)

Reply-To:
emailsecalert1@gmail.com

Date and Time:
3:21 PM Monday 1st June 2020

======
Web Artifacts
======

Full URL (sanitized):
hxxps://outlook-security.emailsecalerts[.]net/index/2020/OWA.php?

Root Domain:
hxxps://emailsecalerts[.]net

======
Investigation
======

Email is themed to look like a security alert from Outlook, claiming the mailbox will be closed unless the recipients confirm their identity. Tells users to click a button. Using Outlook logos.
Reverse DNS search shows that the email has definitely come from Gmail.
URL2PNG shows that the full URL is hosting an Outlook Web Access credential harvester. Requires email and password.
VirusTotal shows this domain has been flagged for malicious/phishing activity.
Checking the SIEM and EDR, no users have clicked on the link and created a network connection to the domain yet.
Checking email gateway shows no users have replied to the email. No other recipients than those stated above.

Domain emailsecalerts[.]net is being used purely for malicious purposes. No legitimate reason for employees to visit this domain. Domain has been alive for 25 days and the name is somewhat typo squatting to make recipients believe it is a legitimate domain related to email security.

Email Description and Artifacts Collected

Sending Address: emailsecalert1@gmail.com

Subject Line: Your Email Will be Locked! Act NOW!

Recipients:
john.smith@dicksonunited.co.uk
alice.cooper@dicksonunited.co.uk
jacon.long@dicksonunited.co.uk
fred.johnson@dicksonunited.co.uk
pickle.rick@dicksonunited.co.uk

Sending Server IP: 209.85.222.173

Reverse DNS: mail-qk1-f173.google.com (Gmail)

Reply-To: emailsecalert1@gmail.com

Date and Time: 3:21 PM Monday 1st June 2020

Full URL (sanitized): hxxps://outlook-security.emailsecalerts[.]net/index/2020/OWA.php?

Root Domain: hxxps://emailsecalerts[.]net

Looking at the reported email in the Outlook email client, this message is impersonating an Outlook security alert using branding such as Outlook logos. The email is informing recipients that their mailboxes will be closed unless they confirm their identity, where they are directed to click on a button, likely leading to a credential harvester based on the context of the email.

Artifact Analysis

Checking the email gateway shows that there have been no outgoing emails to the sending address, therefore no recipients have replied to the sender.

A reverse DNS search on the sending server IP shows that this email has definitely originated from Gmail, and not Microsoft.

URL2PNG analysis shows that the full URL is an Outlook credential harvester, asking users to enter their email and password.

A VirusTotal search for the domain shows that it has been flagged for malicious and phishing activity, therefore it is known to be malicious within the security community.

Checking the SIEM and EDR no employees have made a network connection to the malicious domain, so no recipients have clicked on the link in the email at this time.

The domain is also attempting to typo squat or appear as a legitimate domain related to email security alerts, trying to make the attack more believable to targets.

Suggested Defensive Measures

As the sender is using a Gmail address, the most appropriate action would be to block this specific mailbox to prevent any more incoming malicious emails from this sender.

Requesting an email gateway block for the sending address "emailsecalert1@gmail.com**".**

The domain has been recognized as malicious, and there is no business justification for any employees needing to access this site. As it has a malicious reputation on VirusTotal, and analysis has shown that it is hosting a credential harvester, the entire domain can be blocked on the web proxy, preventing employees from connecting to the site. This will also make future phishing attacks using this same domain ineffective.

Requesting a web proxy block for the domain "hxxps://emailsecalerts[.]net**".**