Project 4
Phishing Report

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.

I. **Reverse DNS** search shows that the email has definitely come from Gmail.
II. **URL2PNG** shows that the full URL is hosting an Outlook Web Access credential harvester. Requires email and password.
III. **VirusTotal** shows this domain has been flagged for malicious/phishing activity.
IV. Checking the **SIEM** and **EDR**, no users have clicked on the link and created a network connection to the domain yet.
V. 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.

Defensive measure

[1] Making to all recipient aware about this "emailsecalert1@gmail.com" . [2] The sending IP revealed it was actually from a Gmail address. [3] Therefore ,blocking the sending server would have a negative impact on the business as legitimate emails would be blocked.

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

[4] The URL was purely create for Phishing/Malicious activities purpose as flagged by VirusTotal. Therefore, there is no business justification for employees to visit it, and we can block the entire domain to prevent employees from visiting .

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