Phishing Attack Write-up

In this attack, we can see that it replicates a real threat from the past.

From our alert, it appears that a phishing attack is being sent to lars@letsdefend.io

Text

Description automatically generated

Let’s check the mailbox and see what the sender has to say.

A screenshot of a computer screen

Description automatically generated

We can see that the grammar is a little off while it appears to be as ambiguous as possible. An attachment is seen, as well. Let’s upload it to VirusTotal and see what the results are.

Graphical user interface, application, Teams

Description automatically generated

VirusTotal is able check the contents, revealing a Trojan. Let’s dig a little deeper.

Graphical user interface, application

Description automatically generated

The hash value offers quite a bit more information if we continue.

Graphical user interface

Description automatically generated with medium confidence

This area checks the hash value against other repositories. This is obviously malicious.

We’ll return to the SIEM and process this alert.

By following a playbook, we can go step-by-step to break it down further. From our research, it appears the e-mail is indeed malicious and unsolicited. Unfortunately, the e-mail made it pass the spam filter and was delivered to the recipient’s mailbox, increasing the likelihood of infection.

In the following screenshot, network logs were checked to see if outbound connections were made to a C2 server.

Table

Description automatically generated

Graphical user interface, text, application

Description automatically generated

As we can see, contact was made to the IP 188.213.19.81 and was allowed.

The security alert can be closed and further reviewed by Level 2 if necessary, as this is a true positive.