BEC –Supply Chain Tip–sheet

Cyanre has observed a new fraud scheme associated with traditional Business Email Compromise (BEC) schemes. The fraud process still remains the same:

- Criminals gain access to a victim's email account
- Change the email inbox rules the so that the criminal can monitor the email account
- Once the criminal obtain contemporaneous and privileged information, the criminal uses that information to induce an unauthorized financial transaction

In traditional Business Email Compromise schemes, criminals attempt to get the victim to make payment into a new/wrong bank account. However, a new scheme is emerging where criminal are getting unknowing victims to send large amounts of product inventory particularly electronics such as laptops, tablets, drones, etc.

In recent weeks, criminals have been targeting electronics vendors using hacked business email accounts from small to mid-scale IT vendors requesting large shipments of electronic inventory. The products are shipped while pending payment through invoices or third party credit financing, but payment is never received. Some of these shipments have been valued as high as R9 million, and a lack of payment can significantly impact these companies ability to continue operations. Once the shipments are received by the criminals, the electronics are fenced through a variety of means and are not recovered by the victim.

There are several warning signs and means of defense against this emerging trend of Business Email Compromise. Warning signs include missing or deleted emails from inboxes, inactive email accounts becoming active again, and calls from vendors and clients claiming solicitation of shipments or change in payment information