United States Secret Service [INFO]

September 9, 2019

[INFO] Information Only Alert – GIOC Reference #19-013-I
TLP Green

Inventory/Invoice Fraud and BEC

The United States Secret Service - Global Investigative Operations Center (GIOC) is observing the emergence of a new fraud scheme associated with traditional Business Email Compromise schemes. The fraud process still remains the same:

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

In traditional Business Email Compromise schemes, criminal actors attempt to get the victim to send wire transfers or ACH payments. However, a new scheme is emerging where criminal actors are getting unknowing victims to send large amounts of product inventory particularly electronics such as laptops, tablets, drones, etc.

In recent weeks, criminal actors 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 $600,000, and a lack of payment can significantly impact these companies ability to continue operations. Once the shipments are received by the criminal actors, 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.

Some practical means of protection to defend against this emerging fraud scheme are as follows:

[INFO] - Indicates informational or educational content.

- Disable any old or unused business email accounts
- Routinely audit email inbox settings for unauthorized installation of email rules to auto-forward or delete emails
- Enable Multi-Factor Authentication for all email accounts to defend against unwanted intrusion
- Call vendors if there is a request for change in bank account information

The US Secret Service is looking for any additional information or incidents similar to that described above. Please reach out directly if you have seen similar activity. The USSS will continue to share information and updates on this activity as it becomes available.

Any questions relating to this alert can be directed to the GIOC at CID.BEC@usss.dhs.gov or 202-406-6009.