Telco/Mobile – Proactive Joint Initiative

Summary: As a regular function within their primary mission, the NCFTA and the FBI's Cyber Initiative & Resource Fusion Unit (CIRFU) based at the NCFTA, regularly seek input from private sector partners, regarding new/evolving Cyber/Digital crime problems they are experiencing. Over the past six months lead by PNC partners within the Security Organization, the FBI, USSS (also based at NCFTA) and NCFTA managers were made aware of account compromises targeting the Mobile channel, resulting in significant losses with funds being stolen via:

- Mobile provisioning – Apple Pay, Samsung Pay
- Zelle real time payments, and
- Card Free ATM cash outs

PNC sought L.E and NCFTA support in convening a working group of effected Banks, and other stakeholders including processors, (EWS, WMC Global) and several Telco/Carriers. The scope of this threat, and significant losses identified by the group lead to increased law enforcement support for developing investigations tied to both the south Florida Haitian gang, as well as the more recently identified Romanian ring, which had previously been tied to significant "Skimming" activity across the United States.

Opportunity for more Pro-active Telco/Carrier support:

Over the past four months PNC (Jess Harrison, Dan Larkin, Jen Gagnon) led efforts, along with FBI and NCFTA to discuss with Telco/Carriers , that are also partners with NCFTA, opportunities to enlist more direct support in identifying criminal SMS Smishing campaigns, that are most often the first steps threat actors engage in, towards compromising mobile devices and/or on line banking credentials. Verizon, AT&T and T Mobile were each engaged separately to encourage more candid discussion, and ascertain certain base capabilities that each carrier might enlist in identifying and interdicting these campaigns. In summary, each Telco advised that they were already seeing ongoing SMS Smishing campaigns and offered several examples of campaigns targeting different organizations, including PNC and many other banks. Following these positive contacts with the Telcos, the FBI and NCFTA offered to convene a Face to Face follow up meeting to further explore a collective view of the larger threat landscape, and to frame the proactive intelligence sharing initiative and answer certain base questions such as:

1) What intelligence is each organization already seeing/sharing ?
2) What additional Intelligence can be shared immediately?
3) How will the intelligence be shared?
4) How/who will store that intelligence?
5) What future opportunities exist for further sharing?
6) What other organizations should be included?

7) Clarify what interdiction and attribution opportunities exist or can be developed

**These questions are not meant to be a comprehensive listing, but are typical questions asked at the outset of any new jointly developed NCFTA initiative.*

Ahead of the Christmas Holidays' the FBI sent out save the dates (with two sets of dates listed) along with a general invitation for the face to face meeting. As responses came back, the best date available was January 23, 2019. The updated invitation with draft agenda was sent out this past Monday (attached).