Ýmsar hættur vegna COVID-19

Europol hefur gefið út aðvaranir á facebook síðu sinni vegna COVID-19 tengt skipulagðri glæpastarfsemi.

Þær ráðstafanir sem gerðar hafa verið á alþjóðavísu vegna COVID-19 hafa orðið til þessa að aðilar sem stunda skipulagða glæpa starfsemi hafa þurft að aðlaga sig að breyttum aðstæðum fljótt. Til að átta sig betur á aðstæðum er mikilvægt er að skoða þær breytingar sem hafa orðið og valdið því að aðilar í skipulagðri glæpastarfsemi beini svikastarfsemi sinni í þessa átt:

- Mikil eftirspurn eftir ákveðnum vörum, hlífðarfatnaði og lyfjum.
- Fólk vinnur meira heima og styðst við ýmsar stafrænar lausnir
- Samkomu takmarkanir gera það að verkum að glæpir eru minna sjáanlegir og færast meira á netið.
- Ótti og kvíði hjá einstaklingum vegna COVID-19 geri þá berskjaldaðari fyrir misnotkun.
- Skortur á ólöglegum varningi í landinu s.s. fíkniefnum getur orsakað ófyrirséðar aðstæður og áður óþekkta brotastarfsemi.
- Mikil tími lögreglu fer í afleiðingar COVID-19

Þegar ofangreint er skoðað verður að hafa í huga að til að ná fram sínu nota glæpamenn tölvupósta, vefsíður, auglýsingar á netinu, síma og skilaboð í hvaða formi sem er til að ná til sem flestra. Þess ber að geta að mikil aukning er á skráningum á lénum sem innihalda corona og COVID.[1] Þessa aukningu má líklega tengja við að svik á netinu aukist.

[1] https://twitter.com/RiskIQ/status/1239619032933748738

Ýmsar hættur vegna COVID-19

Tölvupóstsvik

Tölvupóstsvik felast aðallega í að blekkja einstaklinga til að senda fjármálastofnun eða öðrum aðilum, að því er virðist, eðlileg og lögmæt greiðslufyrirmæli. Þó tölvupóstsvik séu mismunandi eru þau eins að því leiti að búið er að spilla tölvupóstfanginu þ.e. brotamenn hafa stjórn á tölvupósthólfinu eða hafa búið til tölvupóstfang sem líkist tölvupóstfangi sem nýta á. Tilgangurinn með þessu er að fá fjármálastofnanir og/eða aðra til að framkvæma óheimilar og sviksamlegar greiðslur eða senda viðkvæm gögn án leyfis til þriðja aðila sem notar gögnin til að svíkja út fé. Eftirfarandi eru vísbendingar sem geta gefið til kynna að um tölvupóstsvik sé að ræða.

- Viðskiptavinur sendir greiðslufyrirmæli með tölvupósti um að beina greiðslum til þekkts viðtakanda en breyting hefur orðið á reikningsupplýsingum frá síðust greiðslu.
- Viðskiptavinur sendir greiðslufyrirmæli með tölvupósti um að beina greiðslum til viðtakanda sem á enga sögu um greiðslur og engin þekkt viðskiptatengsl við viðskiptavininn. Upphæðin er svipuð eða hærri en greiðslur sem viðskiptavinurinn hefur áður sent.
- Viðskiptavinur sendir greiðslufyrirmæli með tölvupósti um viðbótargreiðslur strax að lokinni greiðslu sem fór inn á reikning sem viðskiptavinurinn hefur ekki áður greitt inn á. Þess konar hegðun getur verið vísbending um að brotamaður sé að reyna að svíkja út enn meira fé því fyrri greiðslan tókst.

Ýmsar hættur vegna COVID-19

- Viðskiptavinur sendir greiðslufyrirmæli með tölvupósti um að færslan sé „áríðandi“, „leynileg“ eða „trúnaðarmál“.
- Viðskiptavinur sendir greiðslufyrirmæli með tölvupósti þar sem gefinn er takmarkaður tími til að framkvæma fyrirmælin og því um leið lítill tími fyrir fjármálastofnanir að skoða umbeðna færslu vel með tilliti til hugsanlegra svika.
- Viðskiptavinur sendir greiðslufyrirmæli um að beina símgreiðslum inn á reikning erlends fjármálafyrirtækis sem hefur verið tilkynntur sem grunsamlegur vegna svikagreiðslna.
- Viðskiptavinur sendir greiðslufyrirmæli sem virðast lögmæt en orðalag, tímasetningar og upphæðir eru ólíkar því sem hefur verið í fyrri greiðslufyrirmælum sem höfðu verið staðfestar og réttmætar.

Fjölþætt athugun fjármálastofnana á greiðslufyrirmælum áður en þau eru framkvæmd kann í mörgum tilfellum að koma í veg fyrir tölvupóstsvik. Til dæmis gætu fjármálastofnanir staðfest greiðslufyrirmælin í tölvupósti og/eða haft samband með öðrum leiðum á sama tíma t.d. símleiðis, á öðrum tölvupóstföngum eða með því að hafa samband við aðra í fyrirtæki viðskiptavinarins sem hafa leyfi til að framkvæma greiðslurnar.

Vefveiðar

Aðilar fara í nokkurs konar veiði herferðir á vefnum þar sem þeir nýta sér ástandið vegna COVID-19 með það markmið að safna persónulegum

Ýmsar hættur vegna COVID-19

upplýsingum eða viðkvæmum gögnum um einstaklinga s.s. aðgangsorðum, notendanöfnum eða greiðslukortanúmerum. Þessir aðilar þykjast jafnvel vera frá þekktum samtökum eða stofnunum t.d. Alþjóðaheilbrigðisstofnuninni.[2]

Fjársafnanir

Einstaklingar eru gabbaðir til að styrkja alls kyns málefni tengd COVID-19 en starfsemin er í raun svikastarfsemi. Settar eru upp vefsíður þar sem notaðar eru falsaðar sögur og myndir af raunverulegu fólk sem hefur enga tengingu við söfnunina. Stundum er notaðar vel þekktar söfnunar vefsíður í þessum tilgangi.

Þekkt eru dæmi um aðila sem hafa gefið sig út fyrir að safna fjármunum vegna COVID-19 en söfnunin hafi svo reynst blekking ein. Sérstaklega ber að sýna aðgát gagnvart alls kyns söfnunum á netinu eða í gegnum síma.

Sala á búnaði sem aldrei berst /sala á eftirlíkingum

Sala á ýmsum búnaði s.s. grímum, hönskum og spritti sem notaður er til að verjast veirunni. Búnaðurinn er jafnvel seldur á heimasíðu sem komið hefur verið upp einungis til þess að svíkja út fé.[3] Mikil eftirspurn er eftir hlífðarbúnaði og öðrum búnaði sem notaður er í heilbrigðisstarfsemi. Þekkt eru dæmi um að slíkur búnaður hafi verið pantaður en aldrei borist.[4]

Einnig er verið að selja hlífðarbúnað og annan búnað vegna COVID-19 sem er eftirlíking og hefur ekki þá eiginleika og gæði sem við má búast. Sala á búnaði sem ætlaður er til heimaprófana á veirunni er áhyggjuefni víða um heim.

[2] https://www.who.int/about/communications/cyber-security
[3] https://www.forbes.com/sites/tedknutson/2020/03/04/marketplace-contagion-amazon-has-already-removed-a-million-fake-products-related-to-coronavirus/#35b33f33418c
[4] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19

Ýmsar hættur vegna COVID-19

Fjárfestingasvik

Varast ber allar fjárfestingar er varða COVID-19 og fjárfestingum þar sem skjótum gróða er heitið.[5]

Berskjaldaðir einstaklingar

Herjað er á aldraða og einstaklinga sem eru haldnir kvíða og ótta vegna COVID-19. Þessir aðilar eru berskjaldaðari en aðrir einstaklingar og freistast frekar til að ýmsan falsaðan varning á netinu t.d. tól til þess að skima sig gegn veirunni heima[6] eða lyf sem eiga að koma í veg fyrir sýkingu.[7] Þekkt eru dæmi um að hringt hafi verið í einstaklinga og þeim boðin meðferð við veirunni.

[5] https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_coronavirus
[6] https://customsnews.vn/fake-coronavirus-test-kits-seized-at-los-angeles-airport-13853.html
[7] https://www.europol.europa.eu/newsroom/news/rise-of-fake-%E2%80%98corona-cures%E2%80%99-revealed-in-global-counterfeit-medicine-operation


MAKE YOUR HOME A CYBER SAFE STRONGHOLD
Á meðan á faraldrinum stendur:
Vertu vakandi og ekki:
EUROPOL
Svara grunsamlegum skilaboðum, tölvupóst-um eða símtölum
Senda peninga til einhvers sem þú þekkir ekki
Kaupa hluti á netinu sem eru uppseldir alls staðar annars staðar
Deila bankaupplýsingum eða öðrum persónulegum upplýsing-um s.s. lykilorði eða notendanafni
Deila fréttum sem koma ekki úr opinberum heimildum
Ekki gefa til góðgerðarstarfsemi án þess að tryggja að um raunverulega starf-semi sé að ræða.
Opna hlekki eða viðhengi í óumbeðnum tölvupóstum og skilaboðum