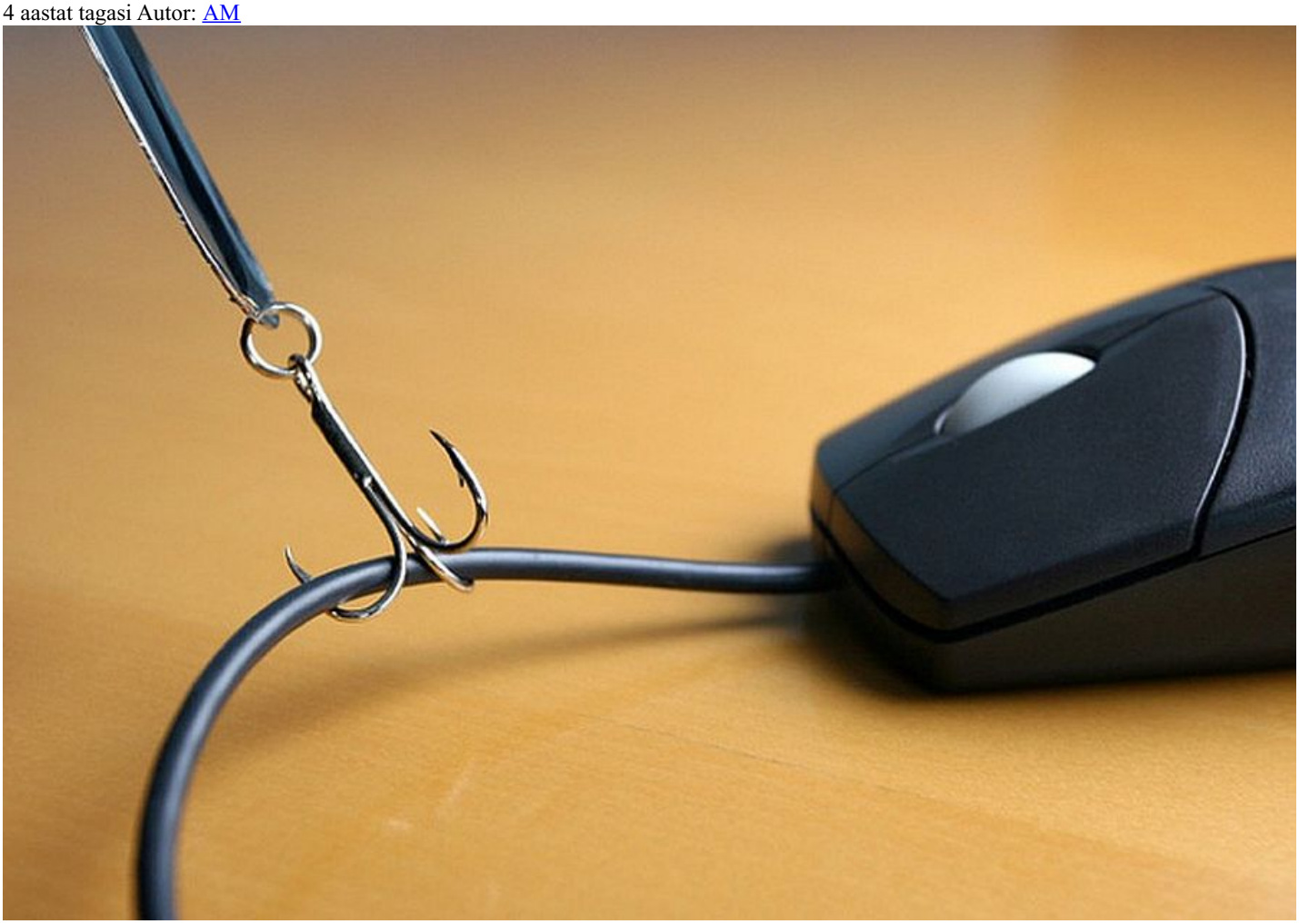
Andmepüügihooaeg: koroonakriisi ajal hakkasid õngitsusrünnetel levima uued nipid

4 aastat tagasi Autor: AM



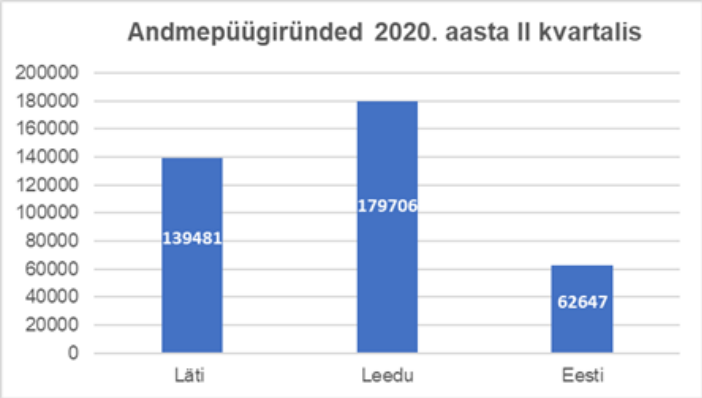
Pärast kevadel alanud COVID-19 nakkuspuhangut on petturid tekkinud olukordi ära kasutades hakanud kasutama uutmoodi andmepüüginippe, millesse on inimestel kerge langeda, kui nad kodust kaupa tellivad või pangaasju ajavad. Koos nendega leitakse ka usutavaid ettekäändeid isikuandmete küsimisel.

Muuhulgas maskeeriti pahaaimamatute kasutajatega suhtlemist, teeseldes järgmiste teenuste osutamist:

- **Kättetoimetamisteenused**. Pandeemia haripunkti ajal kiirustasid kirjade ja pakkide kättetoimetamise eest vastutavad organisatsioonid adressaate võimalikest viivitustest teavitama. Seda tüüpi meile hakkasid petturid võltsima, paludes ohvritel avada manus, et saada teada lao aadress, kust nad saaksid kätte saadetise, mis sihtkohta polnud jõudnud.
- Postiteenused Teine suhteliselt originaalne petturite kasutatud käik oli sõnum, mis sisaldas postikviitungit väikese pildiga. Petturid eeldasid, et huvitatud adressaat aktsepteerib manuse (mille nimi sisaldas küll JPGd, ent mis oli käitus-arhiivifail) täisversioonina ja otsustab selle avada. Nuhkvara Noon leiti postitustest, nagu need, mida Kaspersky teadlased uurisid.
- Finantsteenused Pandeemia tõttu korraldati teises kvartalis andmepüügiründe pankadele sageli meilide kaudu, milles pakuti krediidiasutuste klientidele mitmesuguseid soodustusi ja boonuseid. Kasutajatele saabunud meilid sisaldasid faili koos juhiste või linkidega, et lisaandmeid saada. Selle tulemusel võisid petturid sõltuvalt skeemist saada juurdepääsu kasutajate arvutitele, isikuandmetele või erinevate teenuste autentimisandmetele.
- Personaliteenused Majanduse nõrgenemine pandeemia ajal põhjustas paljudes riikides töötuselaine ja petturid ei jätnud ründevõimalust kasutamata. Kaspersky eksperdid puutusid kokku mitmesuguste postitustega, milles teatati näiteks muudatustest haiguspuhkuse korras või mis üllatasid adressaati uudistega tema vallandamise kohta. Mõnes manuses oli Trojan-Downloader.MSOffice.SLoad.gen fail. Seda troojalast kasutatakse kõige sagedamini krüpteerijate allalaadimiseks ja installimiseks.

„Esimese kvartali tulemuste kokkuvõtmisel eeldasime, et COVID-19 oli viimastel kuudel rämpspostitajate ja andmeõngitsejate põhiteema. Ja nii see oligi. Kuigi oli küll üks harv rämpspostitus, milles pandeemiat ei mainitud, kohandasid andmeõngitsejad oma vanu skeeme nii, et need sobisid parajasti aktuaalse uudistekavaga, ning tulid lagedale ka mõne uue trikiga," kommenteeris seda Kaspersky turbeekspert Tatjana Sidorina.

Kaspersky analüüs näitas, et andmepüügiründed on muutumas üha sihipärasemateks. Samuti on leitud mitmeid uusi trikke – alates personali vallandamisest teatavatest meilidest kuni rünneteni, mis on maskeeritud kättetoimetamisteatisteks. Selliste suundumuste tulemusel on turvalahendused tuvastanud Lätis, Leedus ja Eestis 381 834 andmepüügirünnet.



Isikuandmed hõlmavad finantsandmeid, nagu pangakonto paroolid või maksekaardi andmed või sotsiaalmeedia kontode sisselogimisinfo. Valedes kätes avab see ukse mitmesugustele pahatahtlikele toimingutele, nagu raha varastamine või ettevõtete sisevõrkude ohustamine.

Seda tüüpi ohud on enim mõjutanud Leedu kasutajaid: kolme kuuga avastati seal 179 706 andmepüügirünnet, järgnesid Läti (139 481) ja Eesti (62 647).

Andmepüük on efektiivne ründeviis, sest seda korraldatakse väga ulatuslikult. Seaduslike institutsioonide nime alt massilise meilide saatmise või võltslehtede reklaamimisega suurendavad pahatahtlikud kasutajad oma eduvõimalusi.

2020. aasta esimesed kuus kuud on aga toonud esile selle tuntud ründevormi uue tahu. Tähelepanu äratamiseks võltsisid petturid nende organisatsioonide e-posti aadresse ja veebisaite, kelle tooteid või teenuseid potentsiaalsed ohvrid võisid osta. Nende võltslehtede tekitamise käigus ei üritanud petturid sageli isegi saidist autentset muljet jätta.

Sihipärastel andmepüügirünnetel võivad olla rasked tagajärjed. Kui pettur on saanud juurdepääsu töötaja e-postile, saab ta seda kasutada edasiste rünnete korraldamiseks ettevõtte vastu, kus töötaja töötab, ettevõtte ülejäänud töötajate või ettevõtte lepingupartnerite vastu.

Lisateavet uute andmepüügitehnikate kohta leiab veebisaidilt Securelist.

- Uudised
- Turvalisus