Riigi Infosüsteemi Amet

OHUHINNANG[1]

11. veebruar 2022

Ukraina vastased küberründed ja võimalik mõju Eestis (täiendatud)

Täiendusena 25.01 saadetud ohuhinnangus toodule soovime tähelepanu pöörata kahele peamisele ründevektorile, mida Ukrainas kasutati. Kumbki neist ei ole Ukraina-spetsiifiline, vaid kasutatakse laialt ka mujal maailmas, sealhulgas Eesti asutuste ja ettevõtete vastu suunatud rünnakukatsetes.

1. Ründed teenusepakkuja kaudu

Sellised ründed on oma olemuselt tarneahelaründed – selle asemel, et rünnata asutust x või ettevõtet y, rünnatakse neile it-teenust pakkuvat ettevõtet. Õnnestunud rünnaku korral annab see võimaluse tungida ka teenusepakkuja klientideks olevate asutuste või ettevõtete võrkudesse ning puudulike kaitsemeetmete korral pääseda edasi ka nendesse võrgu osadesse, mis sisaldavad tundlikke andmeid. Kuna teenusepakkuja kaudu võivad ohvriks langeda samaaegselt paljud ettevõtted ja asutused, võib seda tüüpi rünnete puhul potentsiaalne mõju olla suur. Ukrainas oli sihtmärgiks avalik sektor ning rünnati ettevõtet, mis haldas valitsusasutuste veebilehti – ehkki näotustatud veebilehed suudeti kiiresti taastada, õnnestus ründajal tekitada segadust ja hirmu.

2. Ründed lõppkasutaja kaudu

Õngitsusmeilid kasutajatunnuste kätte saamiseks ja pahavara saatmine meilile lisatud manuste abil on jätkuvalt ühed levinuimad ründeviisid, seda nii kuritegelike gruppide kui riiklike ohustajate poolt.

Ukraina kontekstis on taas suurema tähelepanu alla tõusnud just viimased, eriti Vene eriteenistusega seostatud APT Gamaredon (tuntud ka kui Actinium, Armageddon, Primitve Bear). Microsofti teatel on viimane juba alates 2021 oktoobrist aktiivselt sihtinud Ukraina valitsusasutusi, relvajõude, MTÜ-sid, kohtuid ja muid õiguskaitseorganeid. Samuti on sihtmärkide seas organisatsioonid, mis kriisi korral Ukrainas rahvusvahelist või humanitaarabi pakuvad, ning jaanuaris rünnati ka ühe Lääne valitsusasutuse esindust Ukrainas. Rünnete peamine eesmärk on saada kätte tundlikku infot, säilitada ligipääs süsteemidele ja liikuda juba kompromiteeritud organisatsioonide kaudu teiste asutusteni. (Microsoft, BC).

Mõju Eestis

CERT-EE ei ole seni täheldanud Ukraina sündmuste vahetut mõju Eesti küberruumis toimuvale – haavatavuste otsimist ja ärakasutamise katsetamist on näha igapäevaselt, ent mitte tavapärasest erineva käekirja või suurema intensiivsusega.

Arvestades pingelist olukorda Ukrainas soovitame siiski Eesti ettevõtetel ja asutustel üle vaadata ja vajadusel tõhustada küberturbemeetmeid.

[1] 1 1 KüTS'i paragrahv 12: (3) Riigi Infosüsteemi Amet edastab isikutele küberintsidendi ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid.

RIIGI INFOSÜSTEEMI AMET

Soovitused asutuste ja ettevõtete infoturbejuhtidele

1. Lisaks tõhusate meilifiltrisüsteemide ja viirusetõrje rakendamisele soovitame värskendada lõppkasutajate teadlikkust heast küberhügieenist, eriti mis puudutab meili teel levivaid ohte. Olla teadlik, et õngitsuskirjad või ka pahaloomulisi manuseid sisaldavad kirjad võivad olla täpselt sihitud ning näida väga tõepärased (imiteerida rahvusvahelisi organisatsioone, valitsusasutusi vms). Peibutisena võidakse kasutada antud asutuse töövaldkonnaga otseselt seotud teemasid ja / või Ukrainaga seotud teemasid.

2. Kuna ohustajad võivad kasutada meili manusena MS Office dokumente, mis sisaldavad pahavara võimaldavaid makrosid, vaadata üle asutuse makroturbepoliitika. Soovitav on makrod keskselt keelata.

   Makrode kaudu pahavara leviku vastu võitlemiseks astub jõulise sammu ka Microsoft: 07.02 teatas ettevõte, et alates aprillikuistest uuendustest on makrod vaikimisi keelatud nendes failides, mis on veebist või meili teel saadud (st kasutaja ei saa ühe klikiga makrosid lubada). See mõjutab Wordi, Exceli, Powerpointi, Accessi ja Visio failidega saadetavaid makrosid ning rakendub Windows operatsioonisüsteemiga seadmetes.

3. Kaardistada sõltuvused teenusepakkujatest ning ajakohastada välistele partneritele antud ligipääsuõigused ja kontod. Ligipääsu andmisel välistele partneritele tuleks rakendada mitmikautentimist (2FA).

4. Üldise ründepinna vähendamiseks soovitame kaaluda oma IT-taristule veebiliikluse piiramist teadaolevatest anonüümset liiklust võimaldava võrgustiku (TOR) otspunktidest. Meile teadaolevalt kasutatakse TOR võrgustikku asutuste IT-taristute nõrkuste kaardistamiseks, jõurünneteks ja muudeks rünnakukatseteks. Lisaks võimaldab TOR-võrgustik juba paigaldatud pahavara suhtlust juhtserveriga, andmete edastamist ründaja käsutuses olevale serverile jne.

5. Vajadusel / abi saamiseks pöörduda CERT-EE poole.

RIA tegevused

1. Alates 03.02 on RIA tõstetud valmisoleku tasemes.
2. CERT-EE seirab riigivõrgus olevaid asutusi regulaarselt pahaloomuliste, sh riiklike ohustajatega seostatud IP-aadressidelt toimuva liikluse suhtes ja jagab infot vastavates kanalites.
3. RIA küberturvalisuse teenistus pöörab kõrgendatud tähelepanu õngitsuste ja meili teel levitatava pahavaraga seotud teavitustele, eriti avaliku sektori ja ETO-de / OTO-de puhul.

Lisalugemist:

Gamaredoni APT tegevust ja rünnete tehnilisi indikaatoreid on värskelt käsitlenud Palo Alto küberturbeettevõtte uurimisüksuse Unit 42 blogipostitus, samuti Microsofti blogipostitus ning BC artikkel.

CERT-EE poolt 2021 jaanuaris tehtud tehniline analüüs Gamaredoniga seostatud pahavaraga nakatumisest on leitav siin.

Ohuhinnangu koostas RIA analüüsi- ja ennetusosakond koostöös CERT-EE-ga.