RIIGI INFOSÜSTEEMI AMET

OHUHINNANG[1] 11. märts 2022

Ukraina vastased küberründed ja võimalik mõju Eestis

Käesolev täiendab 25.01 ja 11.02 saadetud ohuhinnanguid – mõlemas antud soovitused kehtivad jätkuvalt.

Olukord

Küberrünnakud Ukrainas jätkuvad, ent on jäänud Vene otsese agressiooni ja ohvriterohke sõjategevuse tõttu mõnevõrra tagaplaanile. Massiivseid küberründe elutähtsate teenuste või kriitiliste taristu pihta ei ole toime pandud, esmaste sõjaliste eesmärkide saavutamiseks kasutatakse traditsioonilisemaid viise. Samas toimuvad erinevad küberründed igapäevaselt ja kannavad olulist rolli konflikti osapoolte vahel toimuvas infosõjas.

Peamiselt leiavad aset teenustõkestusründed Ukraina (ja ka Vene) valitsusasutuste veebilehtede ja meediaväljaannete, aga ka finantsasutuste ja teiste organisatsioonide vastu, andmepüügiründed, näotustamised (sisse häkitud veebilehele kuvatakse oma sõnumid, mida soovitakse levitada). Ukraina valitsusasutuste, panga ja muude organisatsioonide võrkudest leiti veebruaris ka uut andmeid hävitavat pahavara (HermeticWiper), mille puhul on tähelepanuväärne, et sama pahavara leidus ka Ukraina valitsusega koostööd tegeva ettevõtte Läti ja Leedu harukontorite võrgust.

Riikide eriteenistuste heaks töötavate või nendega kaudselt seotud ohustajate tegevuse kõrval on käimasolev sõda toonud kaasa massiivse küberaktivismi / häktivismi laine. Aktiivselt tegutsevad nii Ukraina valitsuse juhitud vabatahtlikest koosnev IT-armee (korraldavad peamiselt Vene-vastaseid DDoS ründeid) kui ka rahvusvaheline häkkerite rühmitus Anonymous (on väitnud erinevate Vene propagandakanalite häkkimist ning Vene valitsusasutuste tundlike andmete omamist), Venemaa tegevusele on poolehoidu avaldanud lunavararühmitus Conti. Sotsiaalmeedias liiguvad üleskutsed laiemale üldsusele toetada Ukrainat osaledes erinevates teenustõkestusrünnetes.

Mõju Eestis

Vahetut ohtu Ukrainas toimuv CERT-EE hinnangul Eesti küberruumile senini ei kujuta. Samas võib see olukord kiiresti muutuda, seda enam, et oht konflikti jätkuvaks eskalatsiooniks on suur.

CERT-EE igapäevane monitooring näitab, et haavatavuste otsimine ja nende pahatahtlik katsetamine on tavapärasest pisut aktiivsem. Mõjuga intsidentide arv ei ole senini suurenenud.

Samuti näeme Ukraina ja Venemaaga seotud teemade kasutamist peibutisena:

1) õngitsusmeilide puhul, millega püütakse koguda inimeste andmeid
2) pahavara levitamiseks (meiliga kaasas olev fail nakatab arvuti pahavaraga)
3) petukirjade puhul, kus palutakse inimestelt krüptorahas annetust Ukraina toetuseks (imiteerides näiteks mõnd rahvusvahelist abiorganisatsiooni)

[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.

Samuti tuleb arvestada, et lisaks nähtavatele rünnetele toimub küberruumis pidev varjatud tegevus – ligipääsude otsimine ja juba kompromiteeritud võrkudes vaikselt sees olemine, oluliste andmete tuvastamine. Selle ulatust Eestis on raske hinnata, ent sõltuvalt ründajast võib motivatsioon taolisteks tegevusteks olla käimasoleva konflikti taustal tavapärasest kõrgem.

Üleskutse aidata Ukrainat osaledes DDoS rünnetes erinevate Vene lehtede vastu levis ka Eesti sotsiaalmeedia gruppides, sealhulgas soovitati külastada teatud spetsiaalseid veebilehti ning võimaldada oma seadmes oleval rakendusel (brauseril) osaleda DDoS rünnetes Vene veebilehtede vastu. Lisaks otsestele küberturvalisuse riskidele võib selline DDoS-ide populariseerimise trend tuua kahju ka pikemas perspektiivis ning tuua kaasa teenustõkestusrünnete üldise suurenemise.

Soovitused

1. Praegusel pingelisel ajal peab iga inimene ja iga asutus olema eriliselt tähelepanelik ja rakendama parimaid küberturvalisuse praktikaid. RIA eelnevad avalikud ohuhinnangud koos soovitustega on leitavad siit ning üldsusele suunatud soovitusi saab lugeda siit ja siit.
2. Seoses sotsiaalmeedias ringlevate üleskutsetega osaleda DDoS rünnetes Ukraina heaks tuleb selgitada sellise tegevuse ohtusid. Praktiliselt annab kasutaja oma seadme robotvõrgustiku käsutusse ja käitab tundmatut koodi – mõlemad tegevused on küberturvalisuse seisukohast lubamatud.
3. Kasutades Vene päritolu tarkvara või rakendusi (nt Kaspersky, Yandex) tuleb nende riskid praeguses olukorras uuesti hinnata (eelkõige asjaolu, et nende kogutavad andmed liiguvad Venemaale ja võivad sattuda ka sealsete eriteenistuste kätte). Soovitame vältida nende kasutamist nii töö- kui eraseadmetes.
4. Informeerida kasutajaid, et praegu on liikvel erinevaid libakirju, mis kasutavad peibutisena käimasoleva konfliktiga seotud teemasid (ukrainlaste abistamine, NATO kohtumine, sõjapõgenike logistika jms). Mõned neist võivad olla väga usutavad ja täpselt sihitud konkreetsele asutusele või organisatsioonile. Tundmatuid faile ega linke ei tohi avada ning kahtluse korral tuleb pöörduda oma asutuse kasutajatoe poole. Libakirjadest palume teavitada ka cert@cert.ee

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