

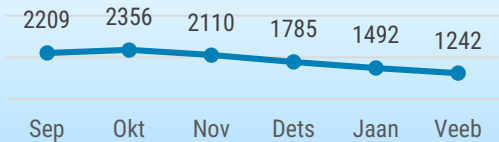


OLUKORD KÜBERRUUMIS

VEEBRUAR 2025

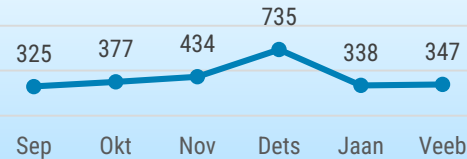
- Veebruaris registreerisime 909 mõjuga intsidenti, mis on viimase poole aasta keskmisest kõrgem näitaja.
- Kahel järjestikusel päeval olid häiritud SMITi teenused, mis mõjutasid häirekeskuse ja politsei tööd. Tallinnas tegutsev ettevõtte sattus lunavararünde ohvriks.
- Korraldasime NB8 CIIP Summiti, kus Põhjamaade ja Balti riikide eksperdid arutasid, kuidas kriitiliselt tähtsate teenuste pakkujaid küberturvalisuse edendamisel paremini toetada. Kirjutasime RIA blogis paroolidest, Signalist ja DeepSeeki võimalustest ning ohtudest.
- New Yorgi MTÜ-d New York Blood Center Enterprises tabas lunavararünnak. Casio Ühendkuningriigi veebipoe lehele oli sokutatud pahavara. Austraalia valitsus keelustas Kaspersky Labi tooted.

Automaatseire: pahavara



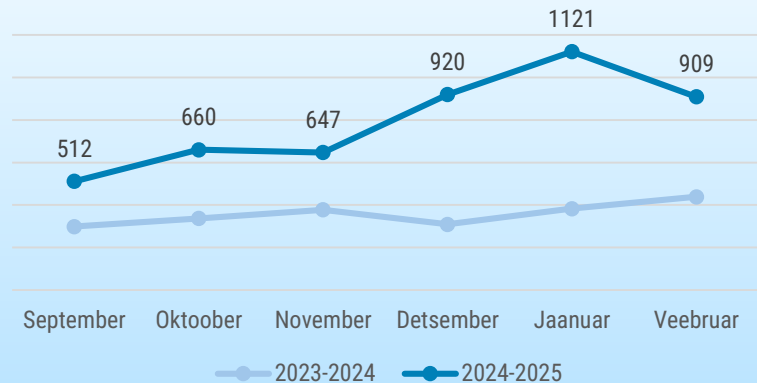
Automaatseire käigus tuvastatud seadmed Eesti küberruumis, mis on pahavaraga nakatunud. CERT-EE teavitab nakatumistest võrkude omanikke.

Õngitsuslehed



Õngitsuslehed moodustavad jätkuvalt suurema osa CERT-EE registreeritud intsidentidest. Alates selle aasta jaanuarist registreerime lisaks petulehti, mistõttu on õngitsuslehtede arv vähenenud.

6 kuu registreeritud intsidendid



CERT-EE-le teavitatud intsidendid, millel oli mõju andmete või infosüsteemide konfidentsiaalsusele, terviklusele või käideldavusele.



Olukord Eesti küberruumis

Veebruaris oli häiritud mitmete teenuste töö.

Muudatuse käigus tekkinud vea tõttu oli 3. veebruaril ajavahemikul 14.10 kuni 15.17 tärkeid Elisa Mobiil-ID töös. 24. veebruaril ajavahemikul 20.36 kuni 21.16 ei töötanud Telia Mobiil-ID teenus. Selle katkestuse põhjus ei ole teada.

3. veebruaril ajavahemikul 11.03 kuni 11.35 ja 23.21 kuni 4. veebruaril 14.57 oli katkestusi veebilehe login.alexela.ee töös. Seetõttu ei saanud kasutajad rakendusse sisse logida ega tasuda Alexela tanklates mobiiliäpiga. Sularaha- ja kaardimaksed toimisid. Intsidendi põhjustas partneri halduses oleva serveri katkestus.

Kahel järjestikusel päeval esines tärkeid SMITi teenustes. 19. veebruaril ajavahemikul 12.58 kuni 13.35 oli häireid hädaabinumbri 112 ja hädaabiteadete menetlemise süsteemis SOS2.

Seetõttu oli osadele hädaabikõnedele vastamise ooteaeg tavapärasest pikem. Intsidendi põhjuseks olid tärked SOS2 andmebaasi töös ebaõnnestunud muudatuse tagajärjel. 20. veebruaril ajavahemikul 8.15 kuni 9.25 ei toiminud piirikontrolli infosüsteem PIKO ega automaatne piirikontrollisüsteem ehk ABC-väravad. Ka selle katkestuse põhjuseks oli ebaõnnestunud tarkvarauuendus, mis häiris andmebaasi tööd.

11. veebruaril krüpteeris lunavara Tallinnas tegutseva ettevõtte videovalve serveris olnud andmed.

Ründajad tungisid süsteemi läbi kaugtöölaua rakenduse (RDP), mida kaitses nõrk parool. Nii nagu ka viimases küberturvalisuse aastaraamatus tõdesime, siis eelmisel aastal tungisid ründajad peaaegu igal kolmandal juhul süsteemi läbi kaugtöölaua rakenduse, kus kasutati nõrku paroole ja puudusid täiendavad turvameetmed nagu VPN, kaheastmeline autentimine, IP-põhised

piirangud, logimine ja monitooring. Soovitame lugeda RIA [ohuhinnangut](#), kus kirjutame kaugtöölaua protokolliga kaasnevatest riskidest ja nende maandamise võimalustest.

Veebruaris levisid taas mitmed erinevad pettused, kuid kõige suuremad kahjusummad tekitati läbi investeerimispettuste.

Investeerimispettuse korral pakutakse ohvrile pealtnäha väga head raha paigutamise võimalust, lubatakse madala riskiga või riskivaba investeeringut ning garanteeritud tootlust. Üldjuhul palutakse raha kanda mõnele kahtlasele krüptovaluutaga tegelevale platvormile ja isikule näidata, et kuidas tema investeering aina kasvab. Seejärel palutakse kanda uus summa ja sama tegevuste jada kordub. Mingil hetkel soovib isik raha välja võtta, kuid see ei ole võimalik. Oleme näinud kahjusummasid, mis ulatuvad mitmekümnete tuhandete eurodeni. Loe ka IT-vaatliku [portaalist](#) samal teemal.



Tegevused küberturvalisuse parandamisel Eestis

Põhjamaade ja Balti riikide eksperdid arutasid Tallinnas 5.02 – 7.02 aset leidnud NB8 CIIP Summitil, kuidas kriitiliselt tähtsate teenuste pakkujaid küberturvalisuse edendamisel paremini toetada. Kuna viimastel aastatel on küberründed tabanud kriitiliste teenuste pakkujaid (pangad, telekomid, haiglad, vee- ja energiaettevõtted), siis on oluline küberohtudega ennetavalt tegeleda. Seetõttu kogunesid RIA kutsel Soome, Rootsi, Norra, Taani, Islandi, Läti ja Leedu küberturvalisuse keskuste esindajad, et vahetada infot parajasti levivatest küberohtudest, jagada kogemusi oma töö tõhusamaks korraldamiseks ning otsida võimalusi veelgi tihedamaks koostööks, mis kulub eriti ära kriiside korral.

Üks levinumaid viise ettevõtete ja asutuste võrkudesse tungimiseks ning sealt info varastamiseks on kasutada mõne töötaja kontot ja parooli. Kirjutasime RIA [blogis](#), kuidas see täpsemalt juhtub ja kuidas on võimalik

end kaitsta.

Kirjutasime lühiülevaate Hiina tehisaru DeepSeek-R1 võimalustest ja riskidest. DeepSeek on väidetavalt suutnud trenida oma keelemudelit võrreldes Lääne analoogidega odavamalt ning vajab ka tunduvat vähem ja nõrgema arvutusvõimsusega kiipe. Peamised mured DeepSeek R-1 mudeli kasutamisel on seotud tsensuuri ning andmete leviku ja kasutusega Hiinas. Loe täpsemalt RIA [blogist](#).

Kuna viimasel ajal on mõnedes artiklites juhitud tähelepanu Signali sõnumirakenduse turvalisusele, kirjutasime sellest lähemalt [blogis](#). RIA hinnangul on Signali kasutamine jätkuvalt turvaline. Rakendus kasutab avatud lähtekoodil põhinevat otspunktide vahelist krüpteerimisprotokollit ja võimaldab verifitseerida sideahela terviklikkust. Pole mingeid viiteid, et rakendust oleks õnnestunud kompromiteerida.

13. veebruaril toimus juba traditsiooniks saanud üritus RIA CyberMeetUp, kus seekord astusid lavale Märt Hiietamm (RIA analüüsi- ja ennetusosakonna juhataja), Kristo Timberg (Hansab ASi tegevdirektor) ja Anto Kallas (TEHIKu infoturbe osakonna juht). Kõigi toimunud ürituste salvestusi saab järgi [vaadata](#). Järgmine üritus toimub 20.märtsil.

Tuletame taas meelde, et juba oktoobris lõpetab Microsoft mitme olulise tarkvara ametliku toe. Alates 14. oktoobrist ei pakuta Windows 10-le turvavärskendusi, uusi funktsioone ega tehnilist tuge. Loe RIA [blogist](#) täpsemalt sel aastal aeguvatest tarkvaradest ja riskidest, mis kaasnevad vananenud tarkvara kasutamisega.

RIA küberturvalisuse aastaraamat on nüüd olemas ka inglise keeles ja sellega on võimalik tutvuda [siin](#).



Rahvusvaheline keskkond

New Yorgi MTÜ-d New York Blood Center Enterprises [tabas lunavararünnak ja keskuse töö täielik taastamine võttis nädalaid.](#) Tegemist on suure verekeskuste ketiga, mis kogub doonoritelt verd ning varustab rohkem kui 400 haiglat 17 osariigis. Intsidendi tagajärjel tuli mitmel pool edasi lükata või tühistada doonorite vastuvõtte vereloovutuseks.

Küberturbe-ettevõtte Trend Micro avaldas [raporti, milles kirjeldatakse Vene häkkerite pahavarakampaaniat Ukraina avaliku ja erasektori asutuste suunal.](#) Kampaania [avastati](#) 2024. aasta septembris ning Trend Micro andmetel kasutasid ründajad turvanõrkust populaarses arhiveerimistarkvaras 7-Zip. Sihtmärkidele saadeti Ukraina valitsusasutusi või eraettevõtteid jäljendav meil, millega kaasas olev manus nakatas avamise korral arvuti pahavaraga. Sel moel õnnestus ründajatel tungida näiteks ühe Ukraina

autotööstusettevõtte, ühistranspordiettevõtte, regionaalse apteegiketi ja veevarustusettevõtte võrku.

Elektronikatootja Casio Ühendkuningriigi veebipoe lehele oli sokutatud [pahavara, mis kogus klientide krediitkaardiandmeid.](#)

Tõenäoliselt kasutati kompromiteerimiseks turvanõrkusi populaarses veebipoodide tarkvaras Magento. Skeem nägi välja nii, et tooted välja valinud ja maksta sooviv klient suunati libalehele, kus ta pahaaimamatult oma kaardiandmed sisestas. Seejärel kuvati veateade ning suunati klient uuesti õigele maksmislehele, kaardiandmed aga olid juba sattunud kurjategijate kätte. Sama pahavaraga nakatati veel vähemalt 16 veebipoodi.

USA-s tegutsev ettevõtte AppSOC, mis tegeleb tehisarurvalisuse ja valitsemise küsimustega, hindas eelmainitud populaarse DeepSeek R1

mudeli turvalisust erinevate parameetrite alusel kokku 6400 testiga ning [leidis, et DeepSeekil puuduvad mitmed olulised turvameetmed.](#) Tõsisemate puudujääkidenähtudega toodi esile DeepSeeki valmisolek luua pahavara või viiruseid. Kokkuvõtteks sai DeepSeek ebaturvalisuse skoori 8.3 10-st, mistõttu ei soovita AppSOC seda organisatsioonidel kasutusele võtta.

Austraalia valitsus [keelustas kõik Kaspersky Labi tooted ja veebiteenused oma süsteemides,](#) tuginedes analüüsile mis väidab, et ettevõtte kujutab riigile märkimisväärset turvariski. Ühendriigid keelustas Kaspersky tooted valitsuse süsteemis 2017. aastal ning laiendas keeldu kõikidele USA firmadele ning tarbijatele 2024. aastal. Ka Saksamaa valitsus ei soovita oma ettevõtetel kasutada Kaspersky tooteid.