Microsofti digikaitse aruanne: maailmas oli 600 miljonit küberrünnet päevas

1 aasta tagasi - 09.12.2024 Autor: AM

Oma iga-aastases digikaitse aruandes, milles käsitletakse suundumusi ajavahemikus 2023. aasta juulist kuni 2024. aasta juulini, toob Microsoft esile küberrünnete murettekitava sagenemise, mis on kaasnenud geopoliitiliste pingete kasvuga. Aruandest selgub, et Microsofti kliendid seisavad iga päev silmitsi 600 miljoni ründega, mille panevad toime nii küberkurjategijad kui ka riiklikult mahitatud ohustajad.

Samuti rõhutatakse, et kübertegevus on tihedalt seotud geopoliitiliste konfliktidega.

„Et küberohtude tulvale tõhusalt vastu astuda, peame oma digikaitset igal tasandil tugevdama ja lisaks võtma endale kindla kohustuse küberturbe põhimõtteid järjepidevalt järgida. See kohustus peab kehtima kõigile alates üksikkasutajatest ja lõpetades ettevõtte tippjuhtkonna ning valitsusjuhtidega, tagades ühtse rinde pahatahtliku kübertegevuse vastu," kommenteeris Microsofti Ukraina esinduse ja Balti piirkonna juht Leonid Polupan.

Aasta suurimad muutused

Microsoft teatas, et lunavararünnete arv kasvas eelmise aastaga võrreldes 2,75 korda, kuid viimasel kahel aastal on enam kui kolm korda vähenenud nende organisatsioonide osakaal, kus on jõutud lõpliku lunaraha maksmiseni (krüptimisstaadiumisse). Ründajad panustavad endiselt ennustatavale inimkäitumisele, näiteks selliste paroolide valimisele, mida on lihtne ära arvata, nende korduskasutamisele mitmel veebisaidil ja andmepüügirünnete ohvriks langemisele. Parooliründed moodustavad 99% kõigist identiteedirünnetest.

Kogu maailmas on sagenenud kübervõimekusel põhinevad finantspettused. Seejuures on uusi suundumusi maksepettustes ning seaduslike teenuste väärkasutamises andmepüügiks ja ründesihiliseks tegevuseks. Üks murettekitav pettusetüüp on techscam ehk tehnopettus, kus kasutajaid petetakse seaduslike teenuste teesklemise või võltsitud tehnilise toe ja reklaamidega. Aastatel 2021–2023 kasvas tehnopettusega seotud liiklus 400%, ületades kaugelt ründevara 180% kasvu ja andmepüügi 30% kasvu. See näitab, et vaja on veelgi

tugevamat kaitset.

DDoS-ründed arenesid jätkuvalt edasi. Aasta teises pooles leevendas Microsoft 1,25 miljonit DDoS-rünnet, mis tähendab eelmise aastaga võrreldes neljakordset kasvu.

Microsofti ohuanalüüs jälgib nüüd rohkem kui 1500 eri ohurühma, sealhulgas enam kui 600 riiklikult mahitatud ohtu, 300 küberkuritegude rühma, 200 mõjuoperatsioonide rühma ja sadu teisi.

Leonid Polupan.

2024. aastal tehti oluline tähelepanek, et haridus- ja teadussektorist on saanud riiklikult mahitatud küberohustajate tähtsuselt teine sihtmärk. Neid asutusi, kust võib saada luureandmeid teadusuuringute ja poliitika kohta, kasutatakse sageli katsepolügoonina enne tegelike eesmärkide kallale asumist.

Geopoliitilised konfliktid on küberkampaaniate ajendiks

Riigid on muutunud kübervaldkonnas agressiivsemaks ja tegevuse tehniline keerukus kasvab pidevalt. See näitab, et üha rohkem investeeritakse ressurssidesse ja koolitusse.

Venemaa, Iraani ja Hiina taustaga ohustajad on intensiivistanud aktiivsete konfliktidega seonduvaid küberoperatsioone. Venemaa ründed on suunatud

peamiselt Ukraina ja NATO riikide vastu, samas kui Hiina on keskendunud Taiwanile ning Kagu-Aasiale. Käimasolev Iisraeli ja Hamasi sõda on hoogustanud Iraani kübertegevust, mille sihikule on võetud Iisraeli, USA ning Pärsia lahe riigid.

Nii Venemaa kui ka Iraan on sõda ja USA valimisi ära kasutanud lõhestava propaganda levitamiseks.

On tuvastatud, et homoglüüfdomeene (sarnase välimusega võltslinke) kasutavad andmepüügiründed on märkimisväärselt sagenenud, kusjuures Microsoft jälgib 10 000 sellist domeeni.

Generatiivse tehisintellekti väärkasutus

Nii küberkurjategijad kui ka riikliku taustaga ohustajad katsetavad tehisintellektipõhiseid töövahendeid. Hiina eelistab kasutada tehisintellekti loodud kujutisi, Venemaa on aga keskendunud tehisintellektipõhistele helitööriistadele. Siiani on need püüded olnud piiratud mõjuga.

Teisest küljest saavad küberturbemeeskonnad tehisintellektipõhiste tööriistade abil kiiremini ohtudele reageerida, automatiseerides selliseid ülesanded nagu hoiatusteadete analüüs.

Kaitse ja koostöö

Microsoft rõhutab, et küberohtude leevendamiseks on vaja avaliku ja erasektori tihedat koostööd. Valitsused peavad rünnete ärahoidmiseks nõudma ründesihilise tegevuse mõjusat karistamist. Kehtivaid rahvusvahelisi norme ei õnnestu küberruumis tõhusalt jõustada ja selle tulemuseks on riiklikult mahitatud agressiooni jätkumine.

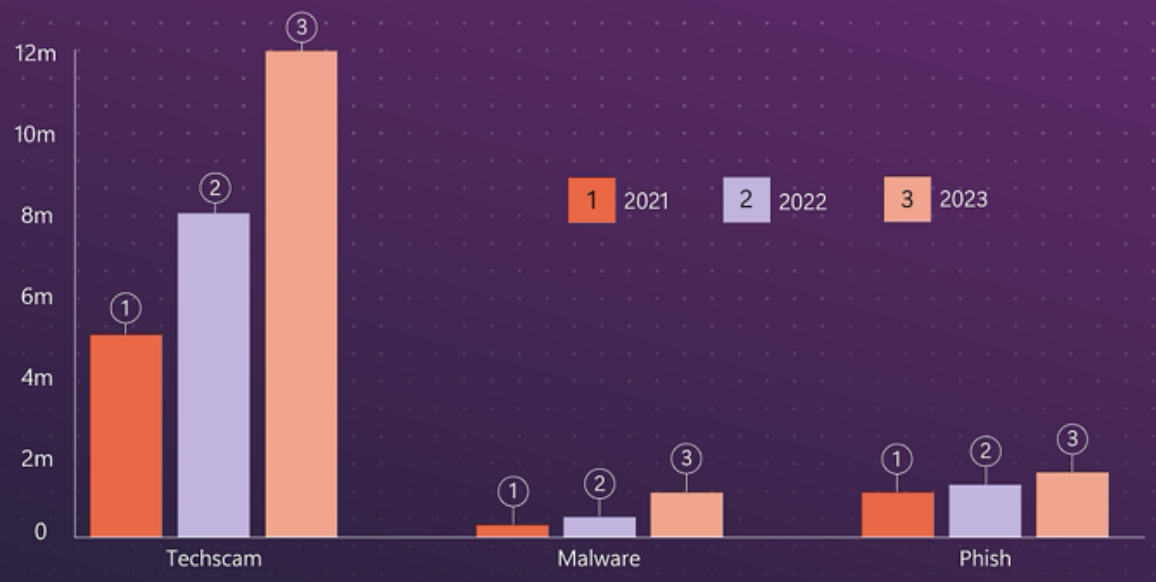
Microsofti turvalise tuleviku algatuse eesmärk on kaitsta kliente digitaristu tugevdamise ja paremate küberturvatavadega. Püsivaks eduks on aga vaja korraga nii kaitset, heidutust kui ka ülemaailmset koostööd –näiteks rahvusvaheliste küberruumis käitumise normide väljatöötamist, et küberrünnete tulva neutraliseerida, soovitatakse aruandes.

- Tegijad
- Uudised

- Turvalisus

Pilt

Daily malicious traffic volume (millions)



The daily volume of techscam traffic has escalated dramatically, skyrocketing by 400% since 2022, a stark contrast to the 180% increase in malware and 30% in phishing over the same period.

Source: SmartScreen log data