

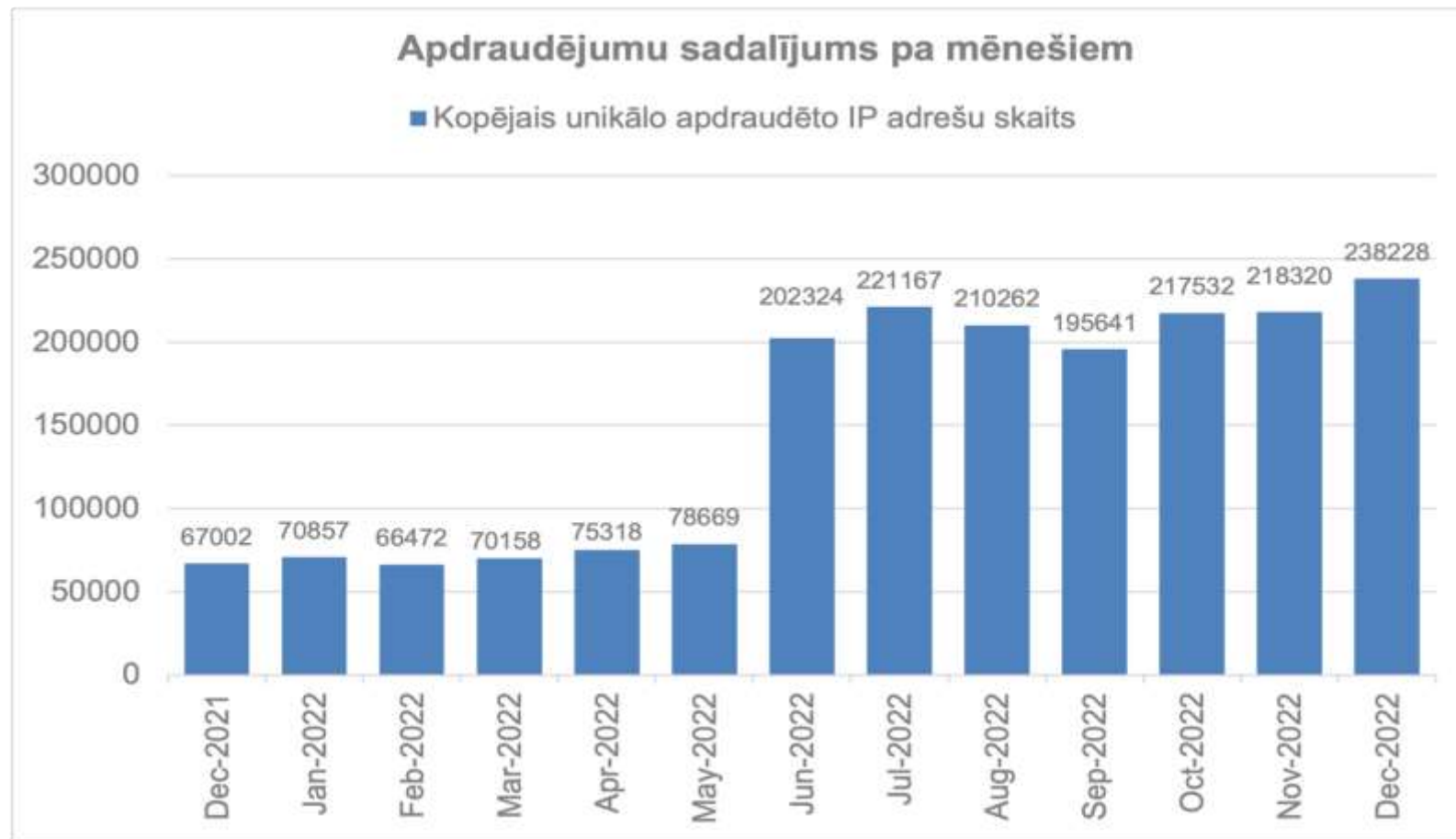
Kiberdrošības situācija Latvijā

Latvijas Pašvaldību savienības sanāksme

20.04.2023. – Egils Stūrmanis, CERT.LV



- Incidentu pieaugums – 40%
- Valsts sektoram uzbrukumu apjoms – x4
- Ievainojamību meklēšana – x7





Valsts soļi brieduma veicināšanā

- Pieņemta jaunā Kiberdrošības stratēģija (2023-2026)
 - Kiberdrošības likums (ITDL vietā)
 - Nacionālā Kiberdrošības centra veidošana
 - MK442 pārstrāde
 - Uzraudzības sistēmas izveide
-




Kas Latvijai uzbrūk?

Krievija realizē plaša mēroga kiberoperācijas vismaz kopš 2007. gada (Agent-BTZ, Turla, ...)

Latvijā kiberdrošības apdraudējuma līmenis noteikts kā augsts kopš 2022. gada janvāra.



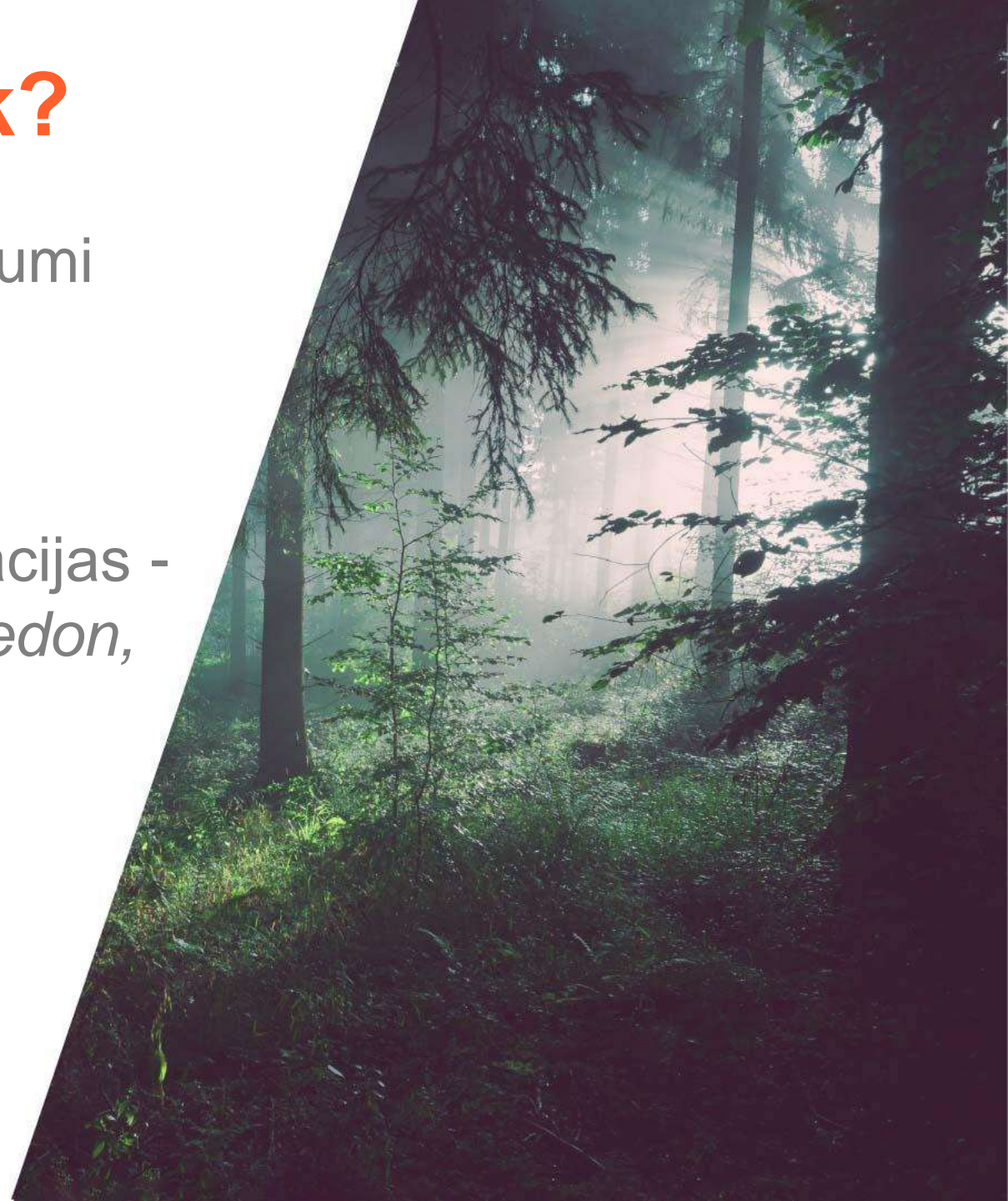
CERT - EU apskats «RUSSIA'S WAR ON UKRAINE: ONE YEAR OF CYBER OPERATIONS»



Poland	22%
Latvia	16%
Estonia	8%
Lithuania	8%
Czechia	6%
Germany	6%
Slovakia	5%
Italy	5%
Finland	4%
France	3%
Hungary	3%
Greece	2%
Romania	2%
Sweden	2%
Other countries*	8%

Kā Latvijai uzbrūk?

- Piekļuves lieguma – *DDoS* uzbrukumi
- Citas haktīvistu aktivitātes
- RU dienestu atbalstītas kiberoperācijas - *Whispergate, Ghostwriter, Gamaredon, Turla...*





DDoS noturība

Esam cienījami pret stāvējuši
apjomīgākajiem un ilgstošākajiem *DDoS*
uzbrukumiem pateicoties



un daudziem citiem partneriem!



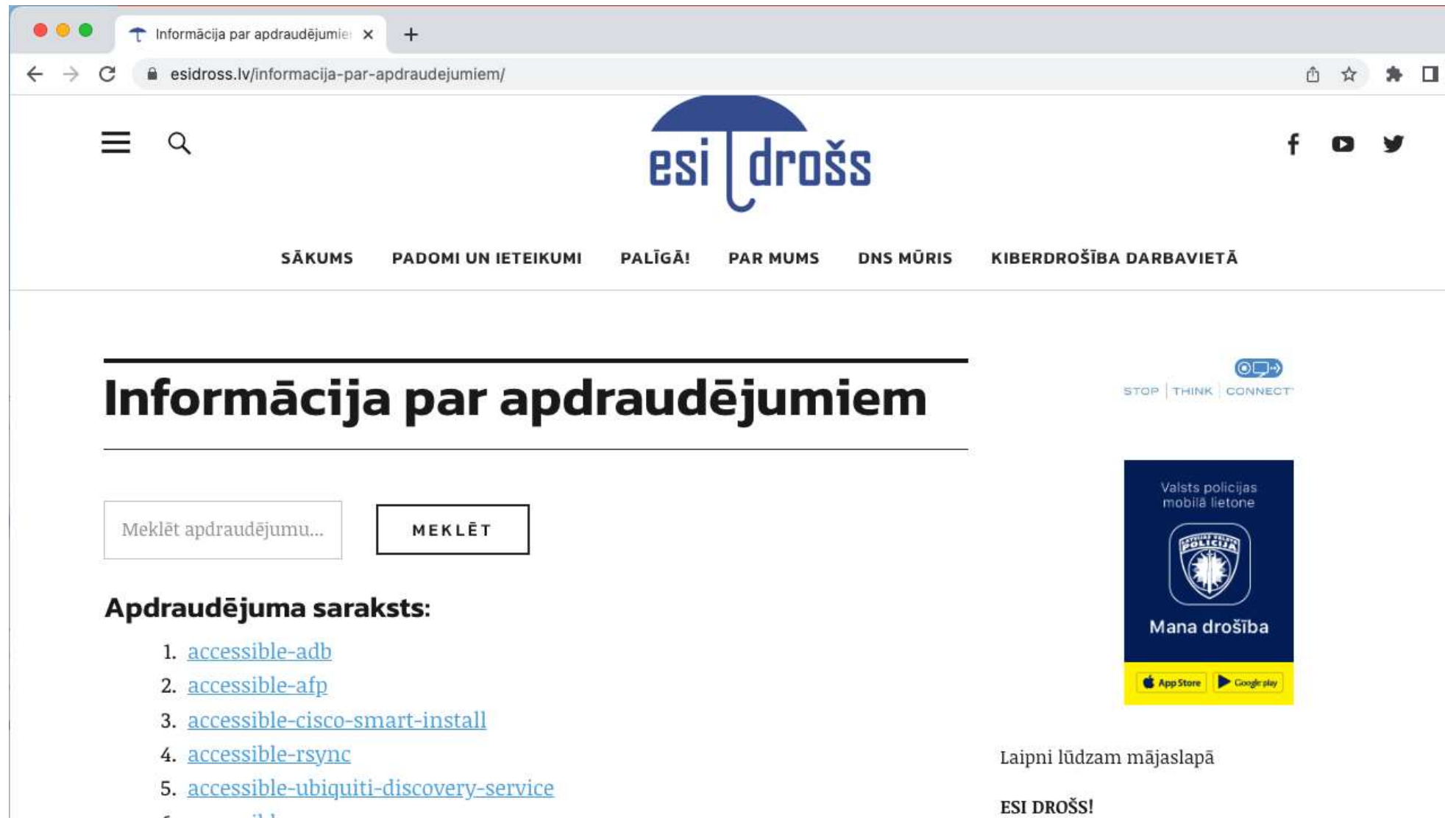


Proaktīvās apziņošanas platforma

Subject: Inficeto IP saraksts [cert@cert.lv] notikumu diapazons [1]
Date: Thu, 30 Mar 2023 09:12:02 +0300
From: cert@cert.lv
To: zina@cert.lv

; CERT.LV ziņojums
; Copyright 2023 CERT.LV. Lauku apraksts:
;
; time - laiks UTC formātā
; ip - avota IP adrese
; asn - avota autonomā sistēma (ja pieejama)
; identifier – apdraudējuma identifikators
; type – apdraudējuma tips
; destination - mērķa IP adrese (ja pieejama)
; destination_port - mērķa ports (ja pieejams)
; destination_asn - mērķa autonomā sistēma (ja pieejama)
; url - saistītā tīmekļa vietne (ja pieejama)
; domain - saistītās tīmekļa vietnes domēna nosaukums (ja pieejams)
; priority - prioritāte (1-zema, 2-vidēja, 3-augsta, 4-ļoti augsta)
; hash - kontrolsumma (izmantojama papildus informācijas iegūšanai <https://www.esidross.lv/cert-lv-bridinajums/?hash/<hash>>)

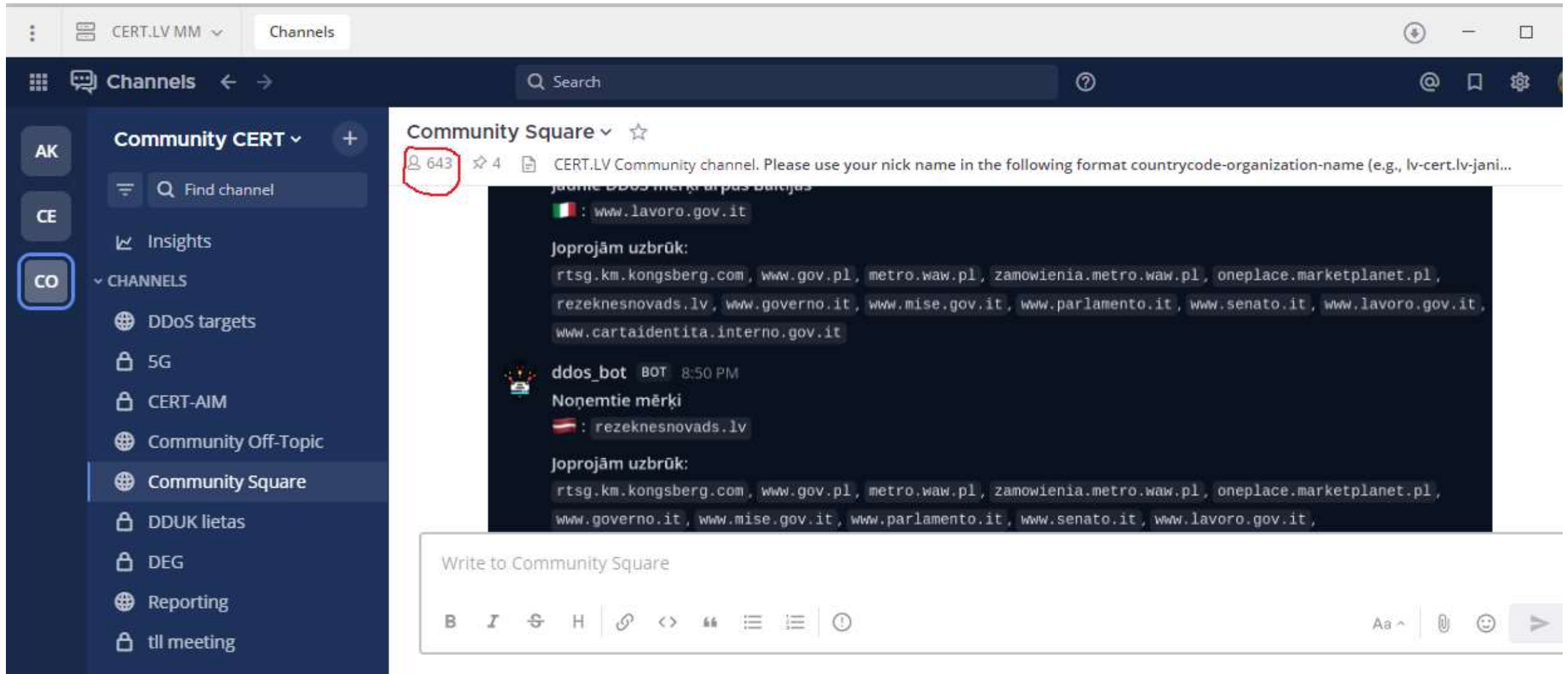
time,ip,asn,identifier,type,destination,destination_port,destination_asn,url,domain,priority,hash
2023-03-28 04:52:04,91.240.x47.x8,29345,accessible-http:http,other,0.0.0.0,,,,,1,hash
2023-03-28 07:22:40,91.240.x47.x9,29345,accessible-http:other,0.0.0.0,,,,,1,hash
2023-03-28 07:22:40,91.240.x47.x9,29345,accessible-http:http,other,0.0.0.0,,,,,1,hash



The screenshot shows a web browser window displaying the website esidross.lv/informacija-par-apdraudejumiem/. The page features a navigation menu with links for SĀKUMS, PADOMI UN IETEIKUMI, PALĪGĀ!, PAR MUMS, DNS MŪRIS, and KIBERDROŠĪBA DARBAVIETĀ. The main heading is "Informācija par apdraudējumiem". Below the heading is a search bar with the placeholder text "Meklēt apdraudējumu..." and a "MEKLĒT" button. A list of links under the heading "Apdraudējuma saraksts:" includes: 1. [accessible-adb](#), 2. [accessible-afp](#), 3. [accessible-cisco-smart-install](#), 4. [accessible-rsync](#), and 5. [accessible-ubiquiti-discovery-service](#). On the right side, there is a "STOP | THINK | CONNECT" logo and a mobile app advertisement for "Mana drošība" by Valsts policijas mobīlā lietone, available on the App Store and Google Play.

Laipni lūdzam mājaslapā

ESI DROŠS!



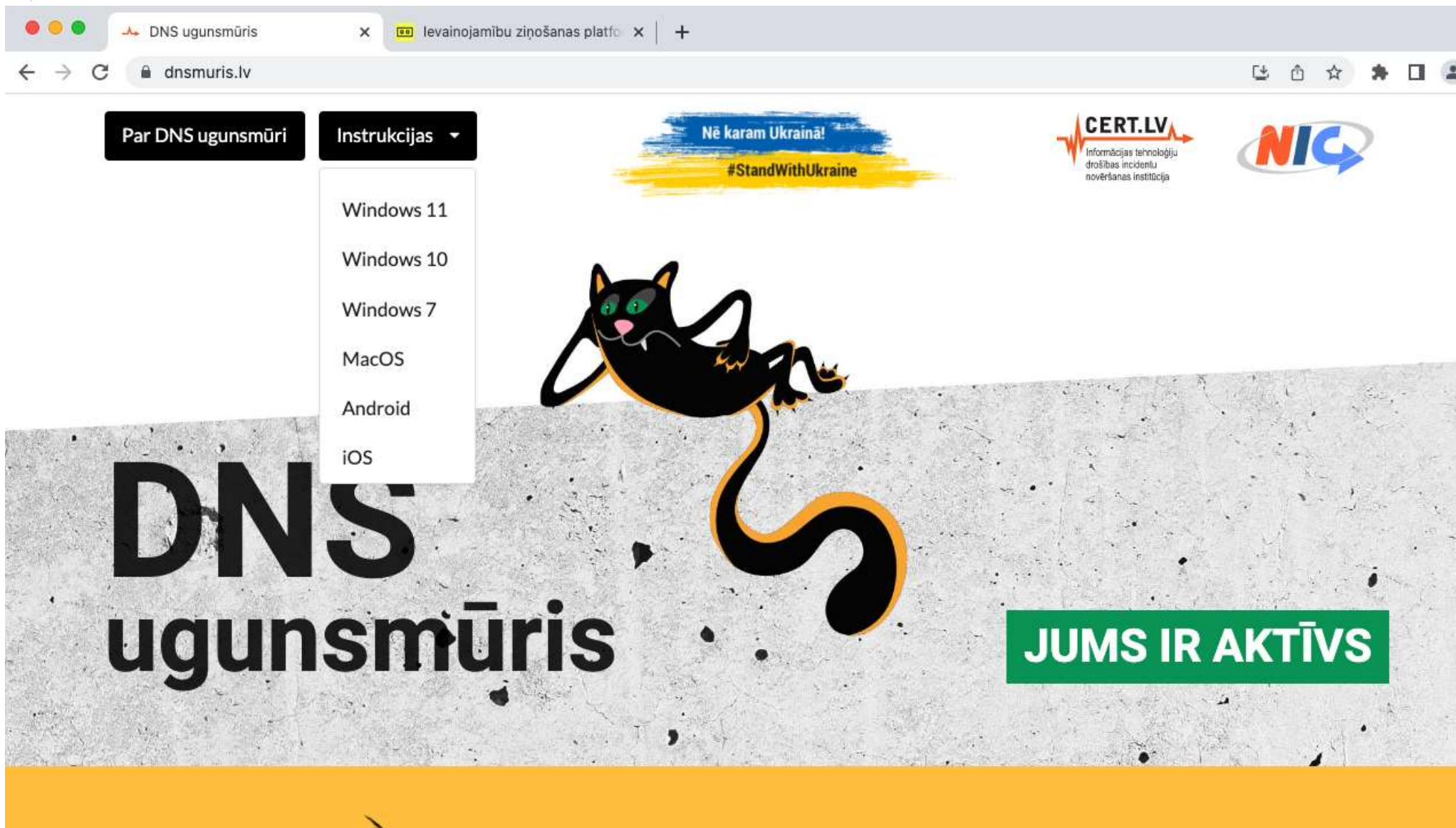
The screenshot shows a Discord interface for the 'CERT.LV MM' server. The left sidebar lists channels under 'Community CERT', with 'Community Square' selected. The main chat area shows a message from user '643' (circled in red) with 4 reactions. The message content is a list of DDoS targets, including:

- rtsg.km.kongsberg.com
- www.gov.pl
- metro.waw.pl
- zamowienia.metro.waw.pl
- oneplace.marketplanet.pl
- rezeknesnovads.lv
- www.governo.it
- www.mise.gov.it
- www.parlamento.it
- www.senato.it
- www.lavoro.gov.it
- www.cartaidentita.interno.gov.it

The message also includes a bot response from 'ddos_bot' with the Latvian text 'Noņemtie mērķi' (Removed targets) and a list of the same targets. The interface includes a search bar, a channel list, and a message input area at the bottom.

CERT.LV Ievainojamību ziņošanas platforma

The screenshot shows a web browser window with the URL `cvd.cert.lv`. The page header features the logo and the text "Ievainojamību ziņošana" (Incident Reporting). Below the header, there are navigation links for "Ziņas" (News), "BUJ" (Help), and "Programmas" (Programs). The main content area includes a breadcrumb trail: "Sākums > Sveicināti CERT.LV ievainojamību ziņošanas platformā!". The main heading reads "Sveicināti CERT.LV ievainojamību ziņošanas platformā!". The text explains that the platform is a state resource for reporting and handling incidents, and that it contains information about participating institutions and programs. It also notes that all reports are registered and that communication is anonymous. A link to `cvd@cert.lv` is provided for reporting. The footer contains the copyright notice "2023 © CERT.LV" and links to "Platformas lietošanas noteikumi" (Terms of Use), "Par mums" (About Us), "Informācija saziņai" (Contact Information), and "Personas datu apstrādes kārtība" (Data Processing Policy).



The screenshot shows a web browser window with the URL `dnsmuris.lv`. The page features a navigation menu with "Par DNS ugunsmūri" and "Instrukcijas" (which is expanded to show a list of operating systems: Windows 11, Windows 10, Windows 7, MacOS, Android, and iOS). A central banner includes a "#StandWithUkraine" message, the CERT.LV logo, and the NIC logo. The main content area has a large "DNS ugunsmūris" title, a cartoon black cat with orange stripes, and a green button that says "JUMS IR AKTĪVS".

Par DNS ugunsmūri

Instrukcijas

- Windows 11
- Windows 10
- Windows 7
- MacOS
- Android
- iOS

Nē karam Ukrainā!
#StandWithUkraine

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

NIC

DNS ugunsmūris

JUMS IR AKTĪVS

Briedums un kiberneturība

- Spējam ātri pielāgoties un mobilizēties
- Strādājam nelielās, taču efektīvās komandās
- Mēs pazīstam viens otru
- Mēs uzticamies un viens otram pierādām, ka varam uzticēties
- Mums ir Kiberaizsardzības vienība Zemessardzē





Paldies!

<https://www.cert.lv>

