# Ceļš ar DNS ugunsmūri

Armīns Palms

14.12.2022

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

# Incidenti

lv- 07:36
hxxps://mooncollege[.]space/tempora/
1

lv- 08:35
mingglessicksel[.]tk - viltus loterijas
1

lv- 12:08
Saņēmu spamu no "Apkalpošana support@email.info.com" ar tēmu "[Netflix] : A
1

lv- 08:50
shrepluses[.]com - viltus loterijas
1

lv- 09:25
hxxps://eu.litbeurope[.]com/ndrS/ - krāpniecība
1

lv- 11:30
Labdien, lūgums ielikt ugunsmūrī šo investment fraud lapu www.linitybase.com
1

lv- 12:41
agidusearheca[.]tk - viltus loterijas

From @inbox.lv>
To cert@cert.lv
Subject **Fake mājaslapa**

Sveiki! Whatsapp lietotnē izplatās links uz CircleK viltus mājaslapu:

https://j0lrft.cyou/noNGBnXy/circlek-2022/?_t=1670259390333#1670414685

| | |
|---|---|
| **Flow Start** | **flow:** 8.8.8.8:53 **time:** 118228 **proto:** udp **local_addr:** 10.127.0.151 **local_port:** 53816 **remote** |
| **DNS Request** | **flow:** 8.8.8.8:53 **time:** 0 **query.0.domain:** www.pyrrhadev.xyz **query.0.type:** IN A |
| **DNS Response** | **flow:** 8.8.8.8:53 **time:** 0 **reply.0.domain:** www.pyrrhadev.xyz **reply.0.type:** IN CNAME **reply.0** **reply.1.answer:** 52.33.207.7 **reply.2.domain:** uixie.porkbun.com **reply.2.type:** IN A **reply.2.answ** |
| **Flow Finished** | **flow:** 8.8.8.8:53 **time:** 118300 **rx_bytes:** 126 **rx_packets:** 1 **tx_bytes:** 63 **tx_packets:** 1 |
| **Flow Start** | **flow:** 52.33.207.7:80 **time:** 118304 **proto:** tcp **local_addr:** 10.127.0.151 **local_port:** 49195 **rer** |
| **HTTP Request** | **flow:** 52.33.207.7:80 **time:** 0 **url:** http://www.pyrrhadev.xyz/oi05/?B8106Fv=ASxi0tQJLFKxMqxq1 |
| **HTTP Response** | **flow:** 52.33.207.7:80 **time:** 0 **response:** HTTP/1.1 307 Temporary Redirect |
| **Flow Finished** | **flow:** 52.33.207.7:80 **time:** 118877 **rx_bytes:** 643 **rx_packets:** 5 **tx_bytes:** 394 **tx_packets:** |
| **Flow Start** | **flow:** 8.8.8.8:53 **time:** 140895 **proto:** udp **local_addr:** 10.127.0.151 **local_port:** 51323 **remote** |
| **DNS Request** | **flow:** 8.8.8.8:53 **time:** 0 **query.0.domain:** www.airstreamsocialclub.com **query.0.type:** IN A |

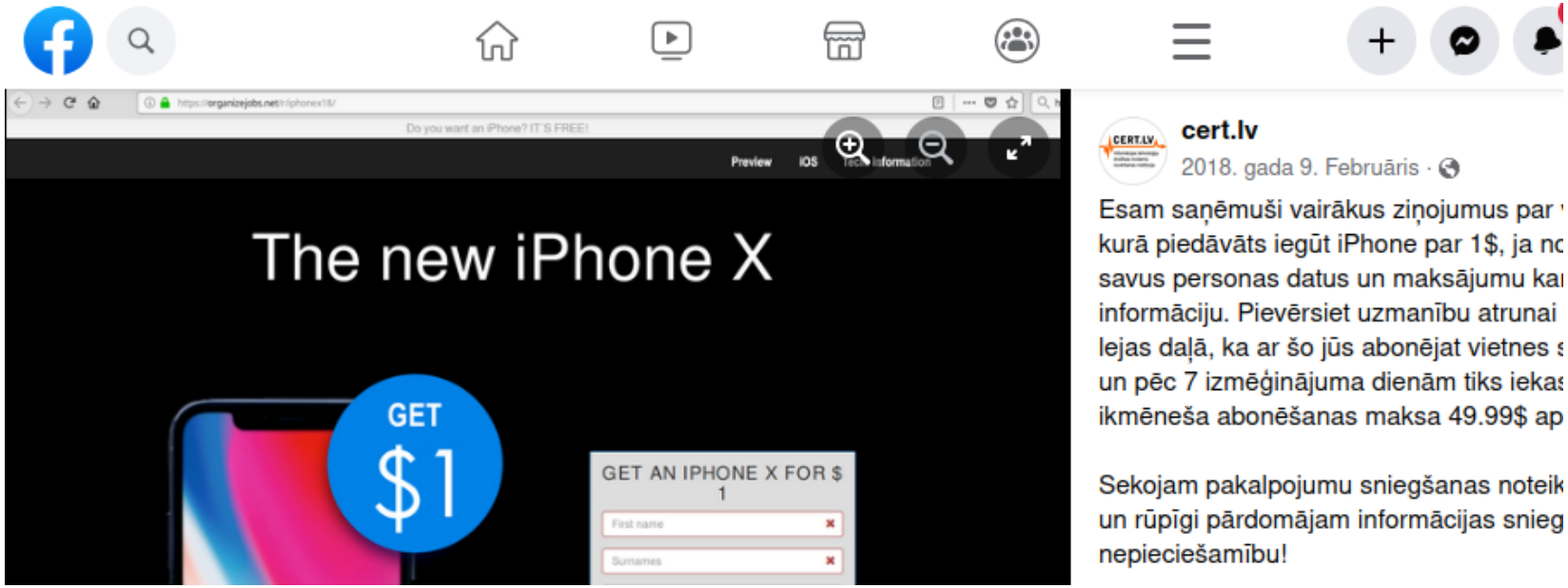
To [redacted] 07.09.16 11:46

Subject **Re: Aizdomīgie domēni**

Labdien,

Parbaudiet arī vai DNS žurnalfailos nav konstatets šāds domēns

dqwdwqwqdqwddqw[.]cn




**cert.lv**

2018. gada 9. Februāris ·

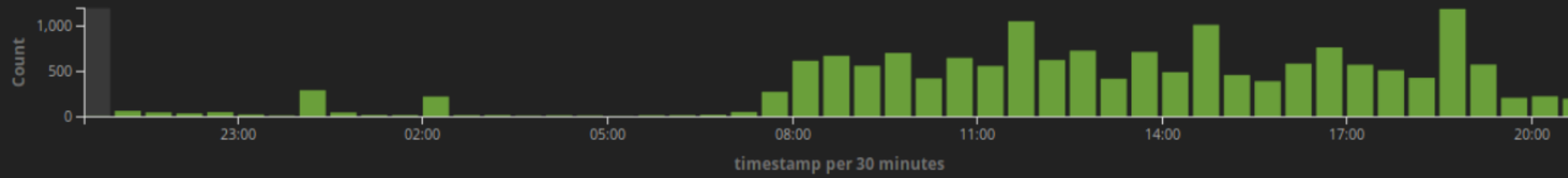
Esam saņēmuši vairākus ziņojumus par
kurā piedāvāts iegūt iPhone par 1$, ja nc
savus personas datus un maksājumu ka
informāciju. Pievērsiet uzmanību atrunai
lejas daļā, ka ar šo jūs abonējat vietnes s
un pēc 7 izmēģinājuma dienām tiks iekas
ikmēneša abonēšanas maksa 49.99$ ap

Sekojam pakalpojumu sniegšanas noteik
un rūpīgi pārdomājam informācijas snieg
nepieciešamību!

Count

16,724
Count

Histogram




Top signatures

| alert.signature.keyword: Descending | Count |
|---|---|
| POLICY Android Device (KitKat OS) Connectivity Check | 5,259 |
| POLICY Android Device (Marshmallow OS) Connectivity Check | 4,254 |
| P2P BitTorrent transfer | 1,800 |
| POLICY TeamViewer DynGate Remote Access Checkin | 1,212 |
| INFO Session Traversal Utilities for NAT (STUN Binding Response) | 946 |
| POLICY HTTP Outbound Request contains pw | 888 |
| MALWARE Suspicious User-Agent (1 space) | 642 |
| P2P BitTorrent DHT ping request | 409 |
| POLICY Dropbox.com Offsite File Backup in Use | 311 |
| POLICY TeamViewer Dyngate User-Agent | 147 |

Export: Raw Formatted

Top categories

| alert.category.keyword: Descending | Count |
|---|---|
| Potential Corporate Privacy Violation | 14,977 |
| Attempted User Privilege Gain | 964 |
| A Network Trojan was detected | 740 |
| Executable code was detected | 25 |
| Web Application Attack | 10 |
| Attempted Administrator Privilege Gain | 8 |

Export: Raw Formatted

Top source IPs

Top destination IPs

# DNS RPZ

- testmalware.lv
- testphishing.lv
- …


*DNS pieprasījums par **kaitīgo** domēnu*

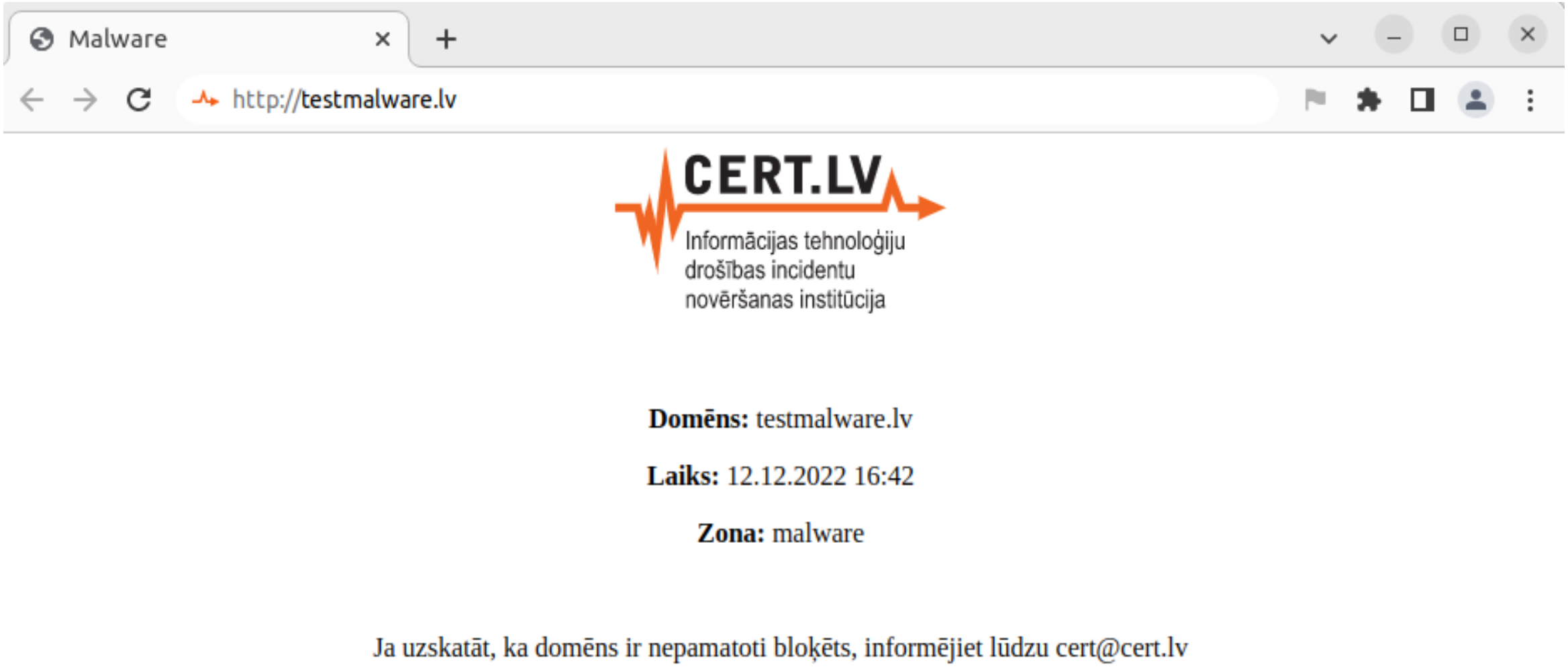
*DNS atbilde ar **drošu** informāciju*

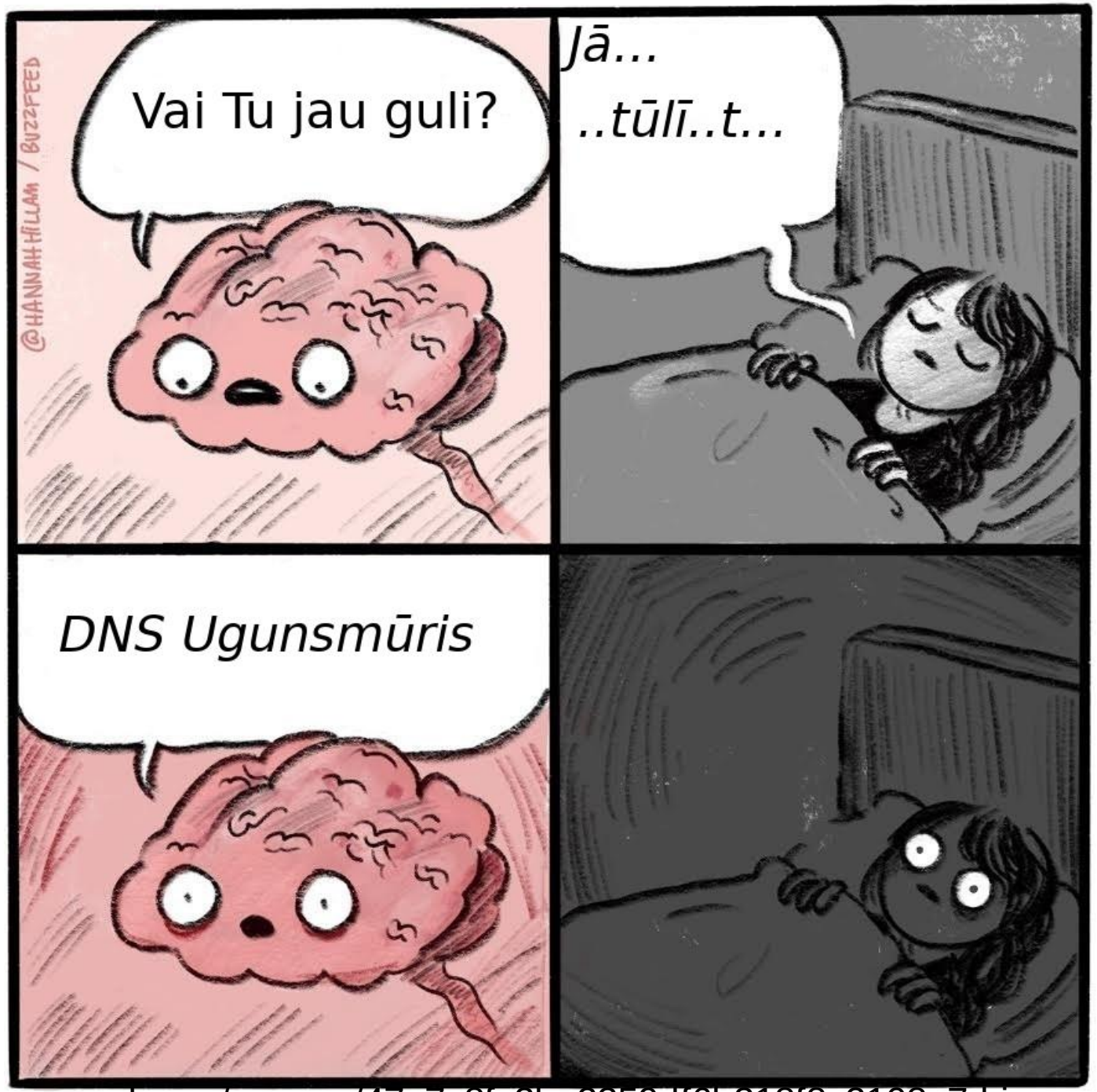
Kaitīga vietne

Pārvirze uz **drošu** lapu

Droša vietne

# Tehniskais nosaukums – RPZ Serveris



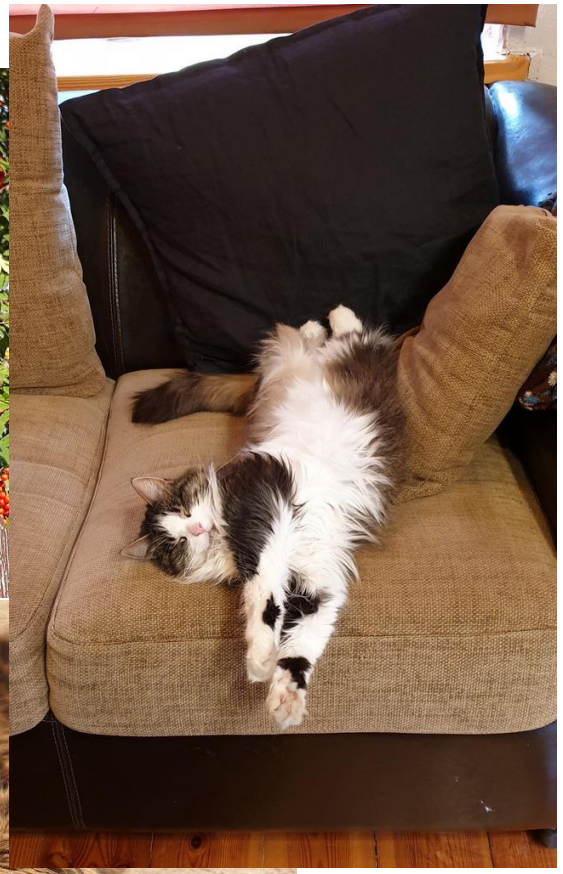


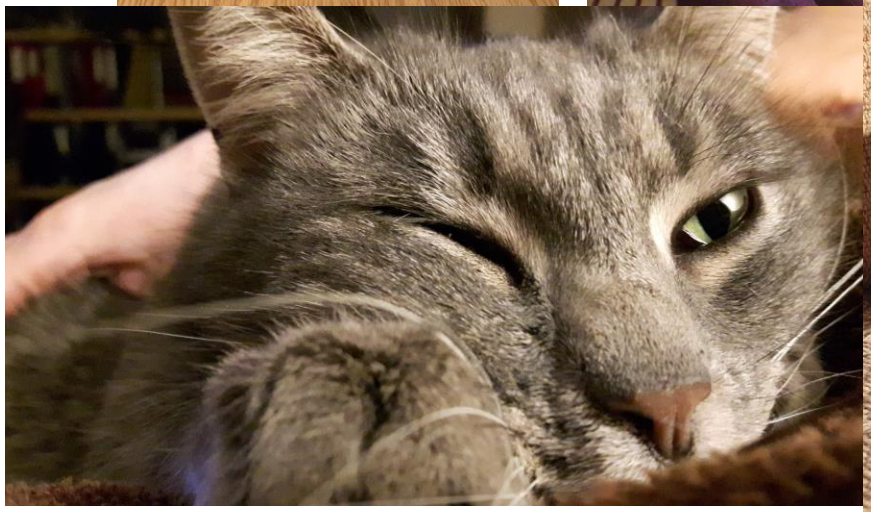

https://www.meme-arsenal.com/memes/47a7c8fc2ba2359df6b318f8c2108a7d.jpg

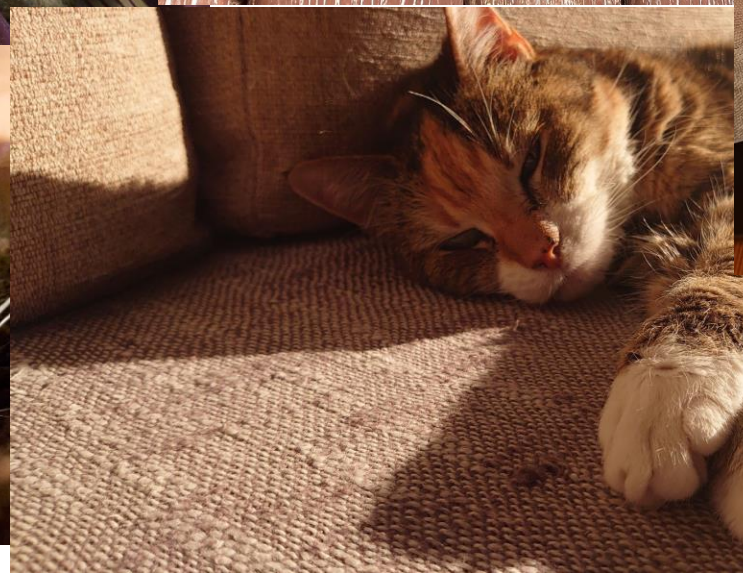
# DNS Ugunsmūra seja

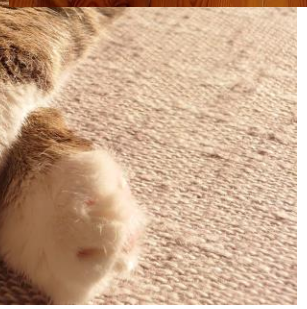
**dnsugunsmuris.lv**

**dnsmuris.lv**







https://dnsmuris.lv

Par DNS ugunsmūri | Instrukcijas

Nē karam Ukrainā! #StandWithUkraine

CERT.LV Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

NIC

# DNS ugunsmūris

JUMS IR AKTĪVS

## Kas tas ir?!

CERT.LV sadarbībā ar NIC (.LV domēna vārdu reģistra uzturētāju) ir izveidojuši DNS ugunsmūri - bezmaksas rīku individuālu lietotāju un organizāciju pasargāšanai no kiberapdraudējumiem, tādiem kā viltus banku lapas, krāpnieciskas tirdzniecības platformas, vīrusus izplatošas vietnes u.c.

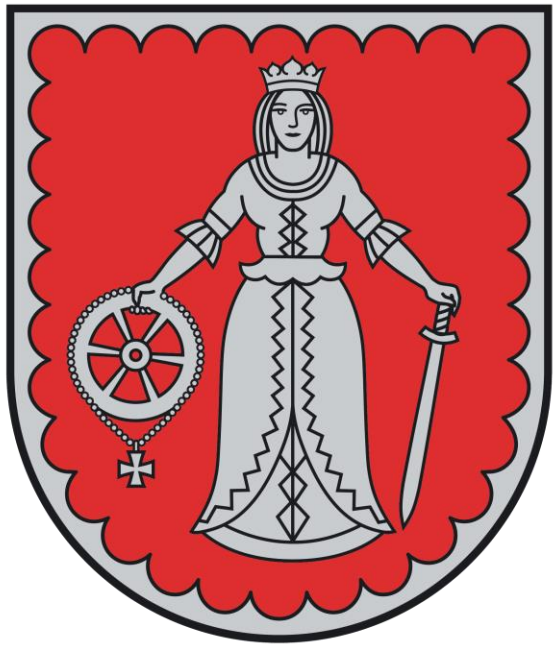
## Lietošana

### DNS ugunsmūra pakalpojums ir BEZ MAKSAS.

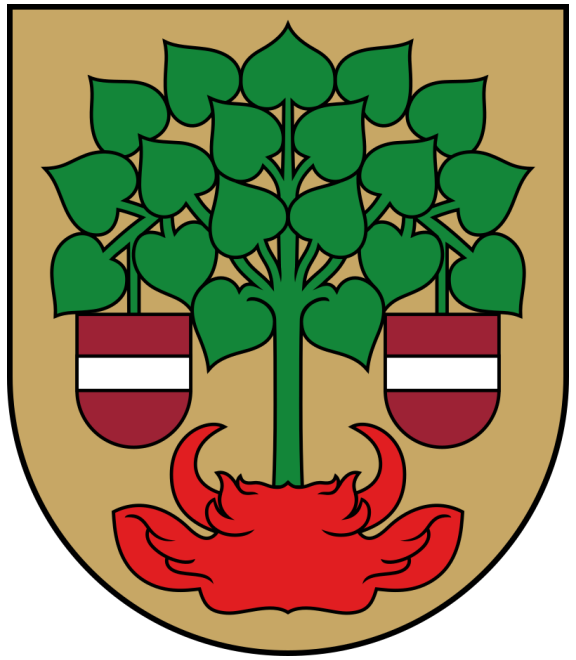
To var izmantot ikviens Latvijas interneta lietotājs (gan mājās, gan darbā). Lai nodrošinātu sev vai saviem klientiem šo papildu aizsardzību, jāizmanto NIC rekursīvie DNS serveri:

IPv4: 91.198.156.20
IPv4: 194.8.2.2
IPv6: 2001:678:84::
IPv6: 2a02:503:8::

# Pirmās pašvaldības



Kuldīga



Valmiera

# Pirmais interneta pakalpojuma sniedzējs

**LMT radījis jaunu kiberdrošības risinājumu “LMT Interneta sargs”**

Reaģējot uz arvien pieaugušo kibernoziedzības apdraudējumu, tostarp Ukrainas karā pielietotajiem hibrīdkara un dezinformācijas paņēmieniem, mobilo sakaru operators un tehnoloģiju inovāciju uzņēmums LMT, izmantojot arī Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas CERT.LV DNS ugunsmūra funkcionalitāti, ir izveidojis jaunu interneta drošības risinājumu “LMT Interneta sargs”. Pakalpojums būs pieejams LMT klientiem, pasargājot gan datoru, gan vie...

# Cik daudz domēnu ievietojam?

01-Dec-2022: info: [RPZ stat info] **163** None -> block
02-Dec-2022: info: [RPZ stat info] **536** None -> block
03-Dec-2022: info: [RPZ stat info] **1358** None -> block
04-Dec-2022: info: [RPZ stat info] **0** None -> block
05-Dec-2022: info: [RPZ stat info] **123** None -> block
06-Dec-2022: info: [RPZ stat info] **383** None -> block
07-Dec-2022: info: [RPZ stat info] **777** None -> block
08-Dec-2022: info: [RPZ stat info] **713** None -> block
09-Dec-2022: info: [RPZ stat info] **655** None -> block
10-Dec-2022: info: [RPZ stat info] **3** None -> block
11-Dec-2022: info: [RPZ stat info] **0** None -> block
12-Dec-2022: info: [RPZ stat info] **536** None -> block

## Kopā: **5247** domēni

# 1 110 311

Tik reizes DNS Ugunsmūris ir apstrādājis kaitīgos domēnu pēdējās 30 dienās

# Atsauksmes



Krāpšana internetā
DNS ugunsmūris (kā pasargāt datoru)
RESUME
10,9 tūkst. abonenti
Abonēt
97
Kopīgošana
Paldies!

## Publiskie DNS serveri

Datoru lietas  Perifērijas ierīces un tīkla tehnika

**fufcix** #4 February 9, 2021, 10:11am

uzliku vietējo pamēģināt, domājot par drošību
dnsmuris lv
IPv4: 91.198.156.20
IPv4: 194.8.2.2

**Jēkabs** 24.01.2022 09:17

Savulaik uzstādīju mājas rūterim https://dnsmuris.lv/. Pagaidām nostrādājis ir tikai vienreiz, kad speciāli apmeklēju lapu, lai redzētu, ko tad parāda.

4 Atbildēt

**NIC.LV - Tavs domēns** Arī DoT pieeja un dnssec validācija. Starp citu, NIC DNS serveriem ir visātrākais reakcijas laiks, pat pārspējot populāros 8.8.8.8 un 1.1.1.1. Sekojošā attēlā var redzēt pēdējo 24h monitoringu no Mikrotik Dude monitoringa sistēmas. Tiek mērīts tieši DNS pieprasījuma laiks un atbilde, nevis pings.


CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija
DNS
ugunsmūris

CERT.LV

# Paldies!

dnsmuris.lv

armins.palms@cert.lv

certlv

certlv