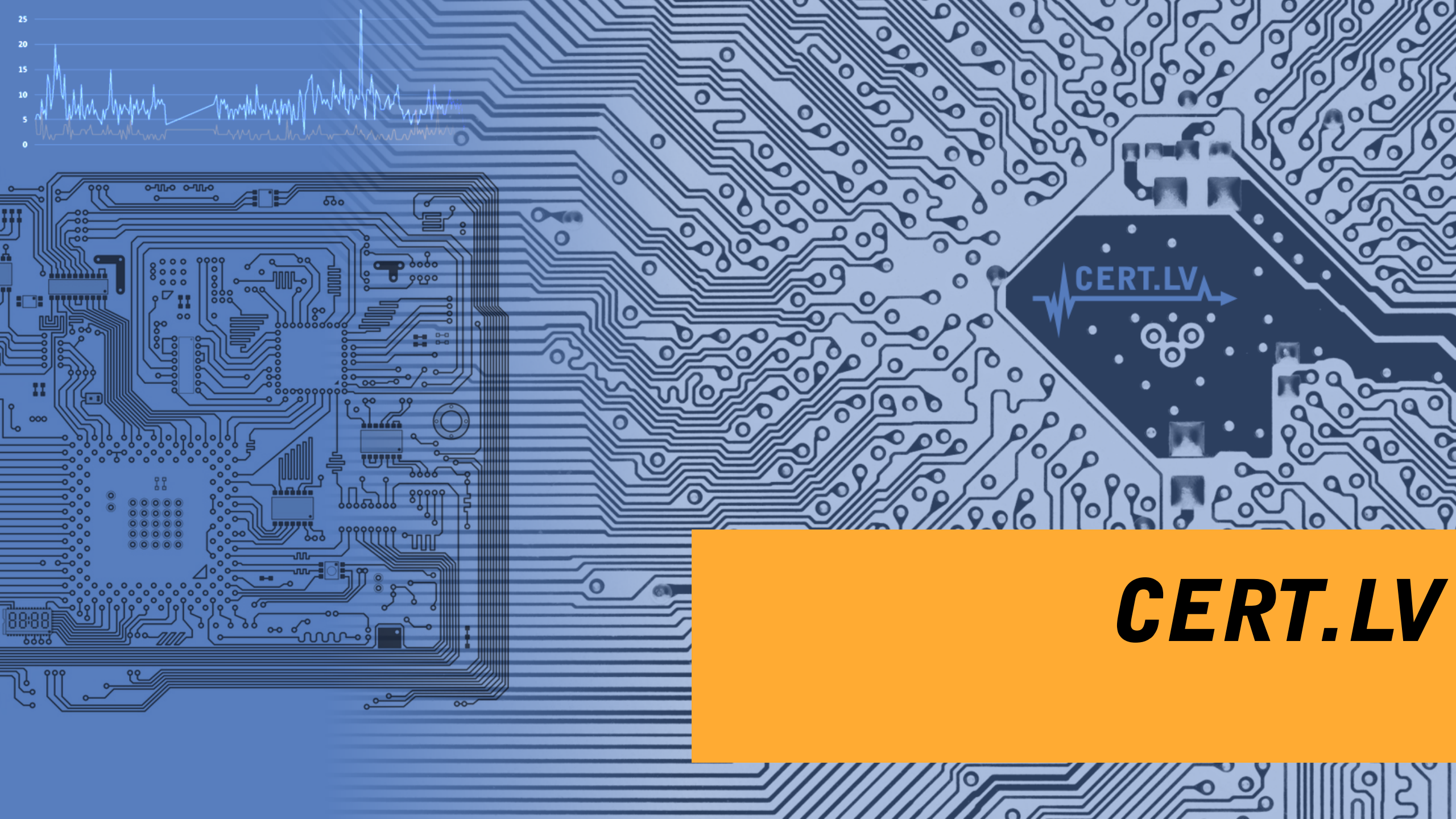
CERT.LV

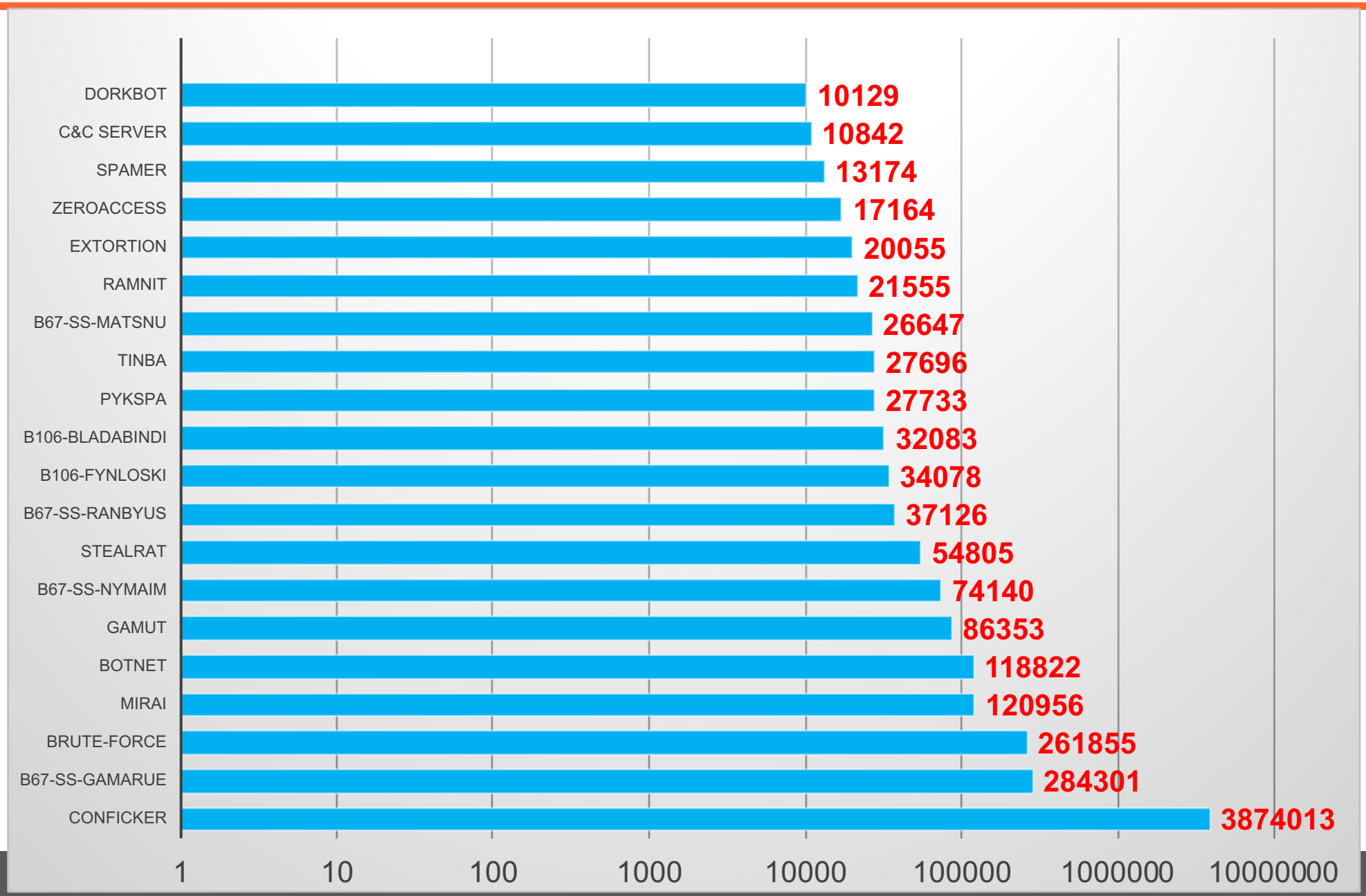
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

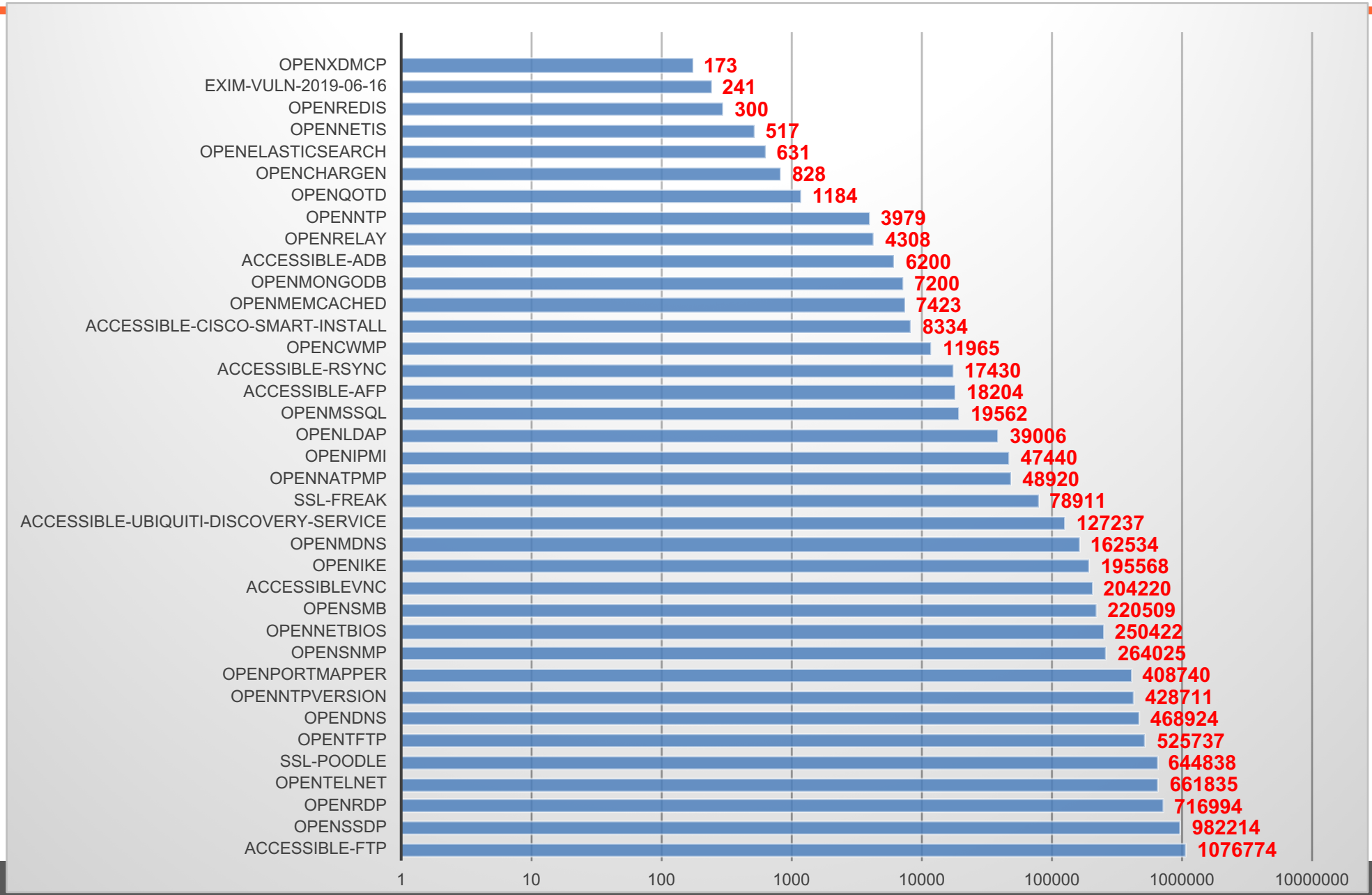
Inficētu iekārtu radītās problēmas

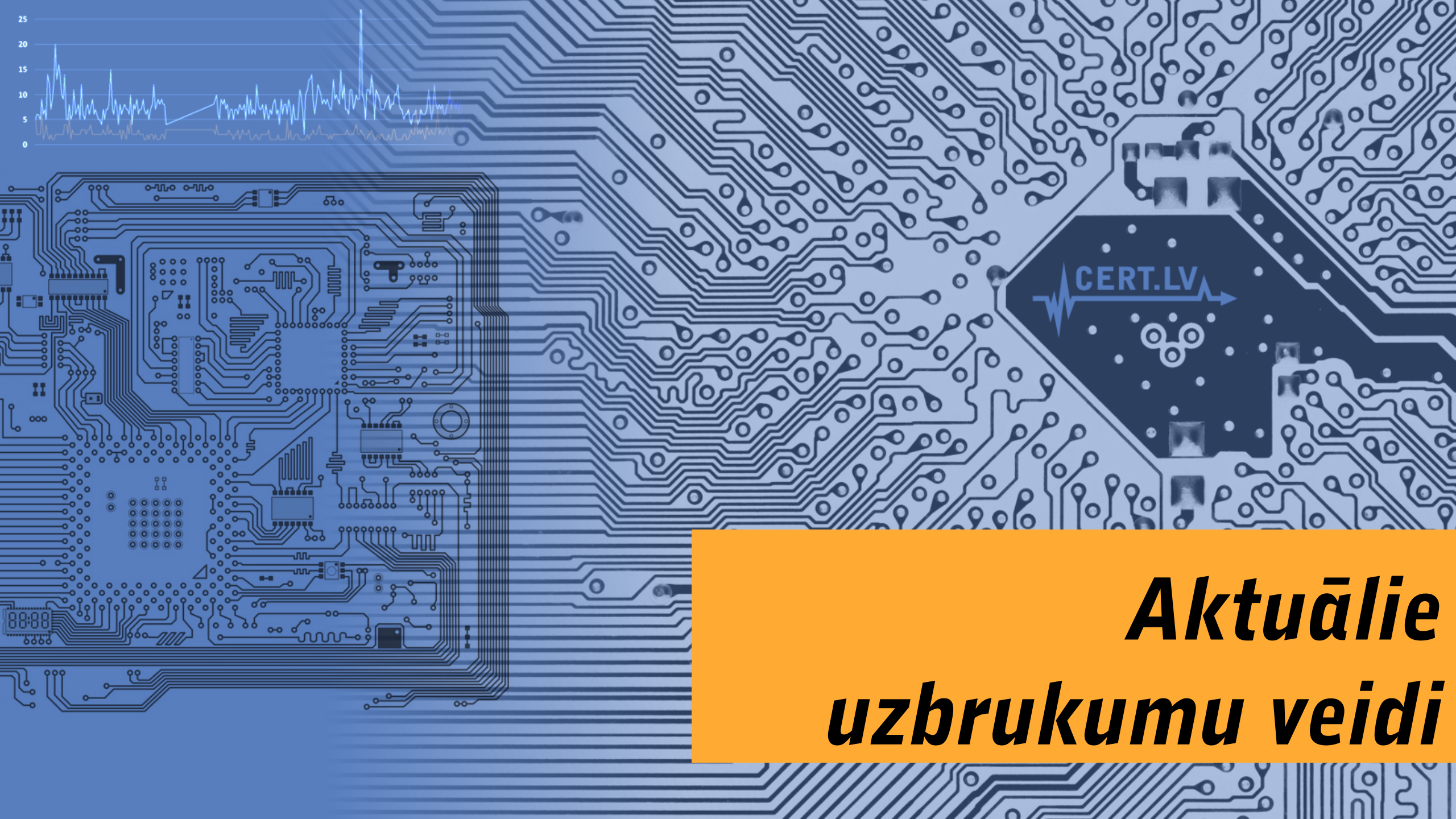
28.11.2019.
Gints Mālkalnietis



CERT.LV


DORKBOT
10129
C&C SERVER
10842
SPAMER
13174
ZEROACCESS
17164
EXTORTION
20055
RAMNIT
21555
B67-SS-MATSNU
26647
TINBA
27696
PYKSPA
27733
B106-BLADABINDI
32083
B106-FYNLOSKI
34078
B67-SS-RANBYUS
37126
STEALRAT
54805
B67-SS-NYMAIM
74140
GAMUT
86353
BOTNET
118822
MIRAI
120956
BRUTE-FORCE
261855
B67-SS-GAMARUE
284301
CONFICKER
3874013
1
10
100
1000
10000
100000
1000000
10000000


OPENXDMCP 173
EXIM-VULN-2019-06-16 241
OPENREDIS 300
OPENNETIS 517
OPENELASTICSEARCH 631
OPENCHARGEN 828
OPENQOTD 1184
OPENNTP 3979
OPENRELAY 4308
ACCESSIBLE-ADB 6200
OPENMONGODB 7200
OPENMEMCACHED 7423
ACCESSIBLE-CISCO-SMART-INSTALL 8334
OPENCWMP 11965
ACCESSIBLE-RSYNC 17430
ACCESSIBLE-AFP 18204
OPENMSSQL 19562
OPENLDAP 39006
OPENIPMI 47440
OPENNATPMP 48920
SSL-FREAK 78911
ACCESSIBLE-UBIQUITI-DISCOVERY-SERVICE 127237
OPENMDNS 162534
OPENIKE 195568
ACCESSIBLEVNC 204220
OPENSMB 220509
OPENNETBIOS 250422
OPENSNMP 264025
OPENPORTMAPPER 408740
OPENNTPVERSION 428711
OPENDNS 468924
OPENTFTP 525737
SSL-POODLE 644838
OPENTELNET 661835
OPENRDP 716994
OPENSSDP 982214
ACCESSIBLE-FTP 1076774
1
10
100
1000
10000
100000
1000000
10000000



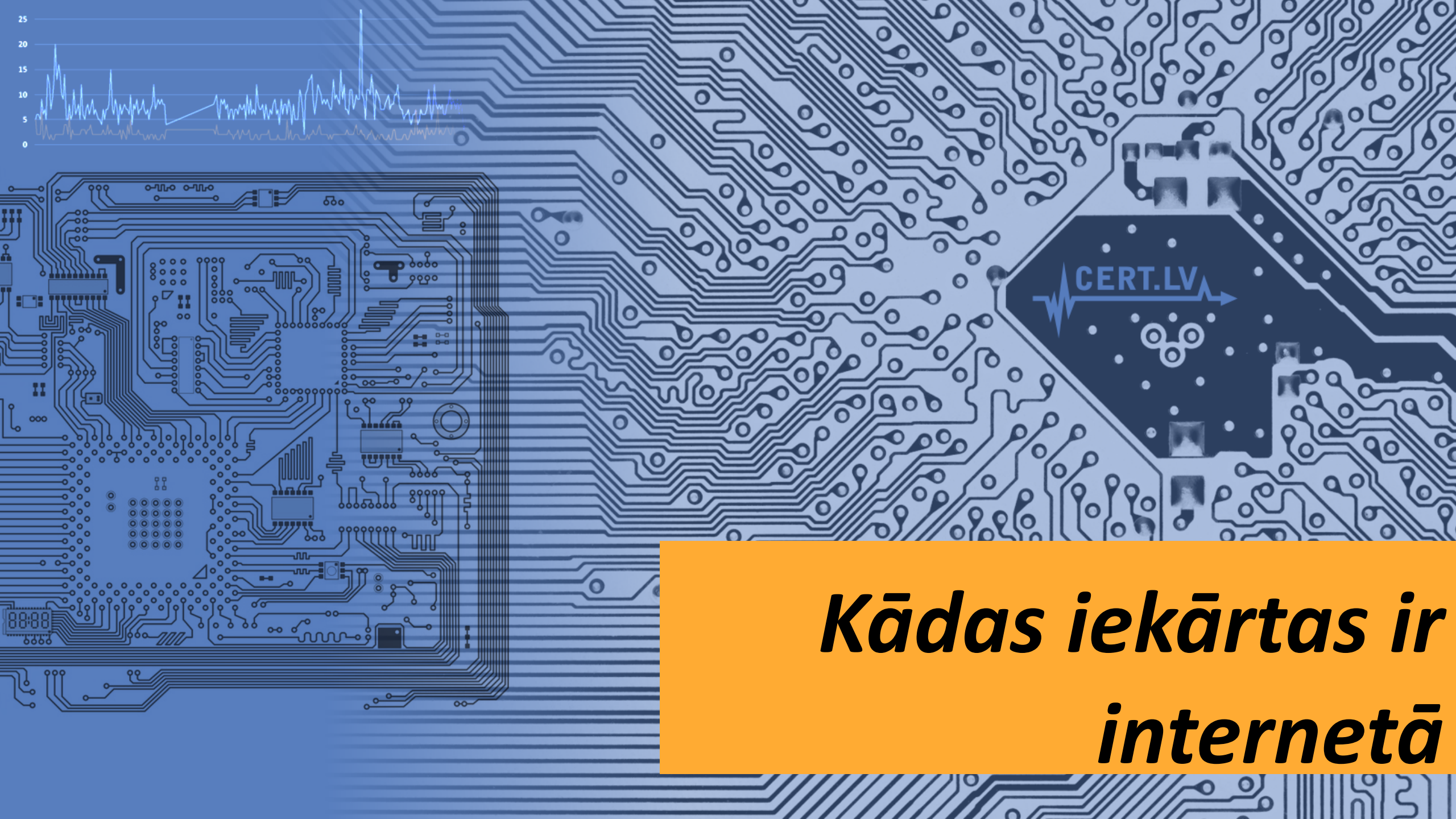
Aktuālie uzbrukumu veidi

Kāpēc uzbrukumi ir sekmīgi?

1. Vājas paroles
2. Neeksistējošs/nepietiekams monitorings
3. Nav veikta pietiekama piekļuves tiesību nodalīšana
4. Steiga ieviešot jaunus pakalpojumus, bez adekvātu drošības risinājumu izvēles
5. Datortīkla un tajā esošo servisu uzbūves nepārzināšana
6. Nepietiekama programmatūras versiju/atjauninājumu kontrole un ievešana

«Svarīgi» un ‘nesvarīgi’ uzbrukumi

1. Automatizēti uzbrukumi un ievainojamību meklēšana notiek nepārtraukti
2. Uzņēmuma lielums, tirgu daļa utt. nekādi neietekmē automatizētus uzbrukumus!
3. Datortīkla aizsargsistēmām jādarbojas vairākos līmeņos
4. Skaidri jāsaprot kuri procesi ir KRITISKI svarīgi, un jāapzin to darbībai nepieciešamo resursu kopu
5. Biznesa procesi ir vairāk saistīti ar datorsistēmām kā šķiet



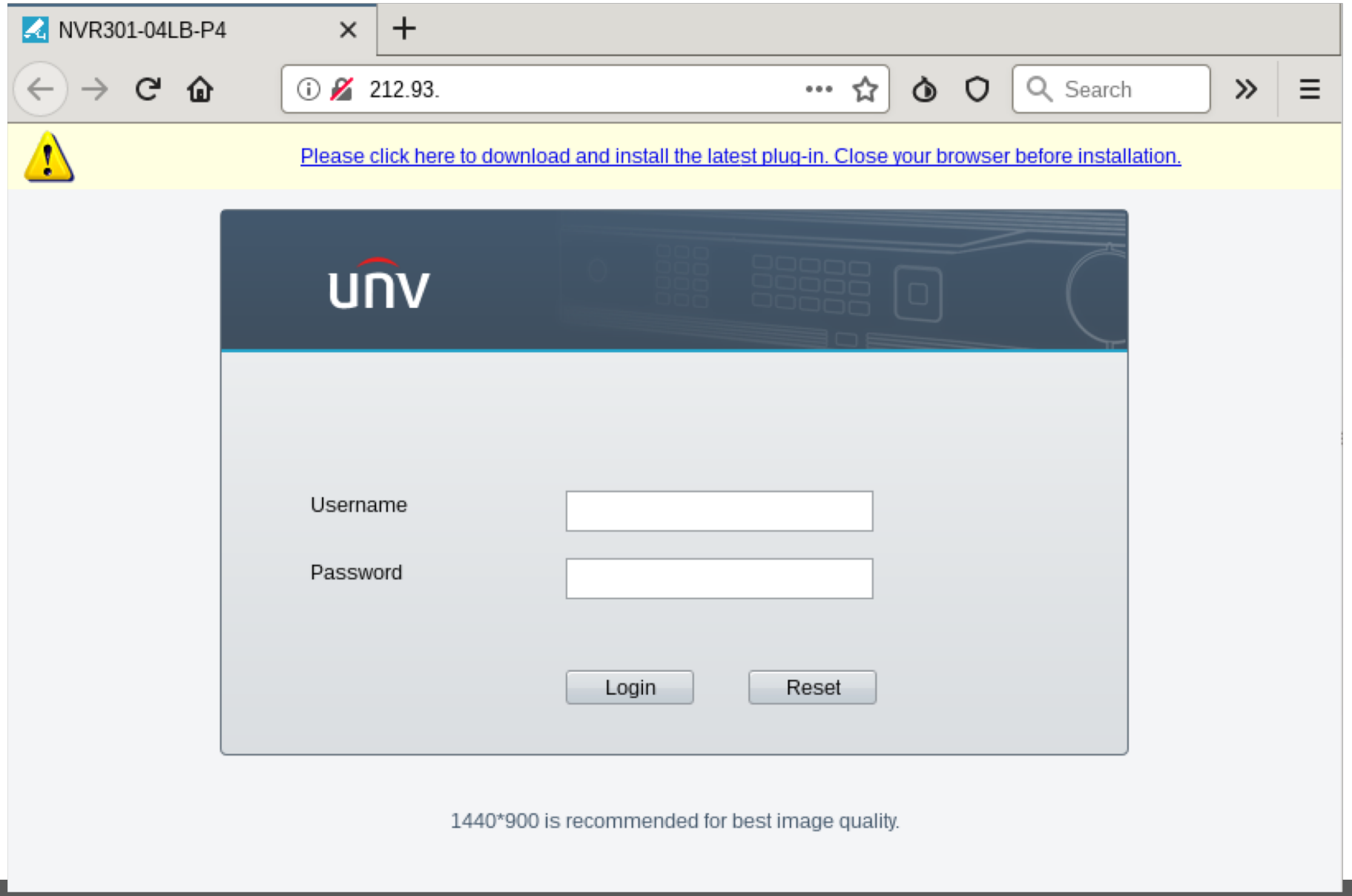
Kādas iekārtas ir internetā

Biežāka inficētās -IOT – aizmirstās iekārtas

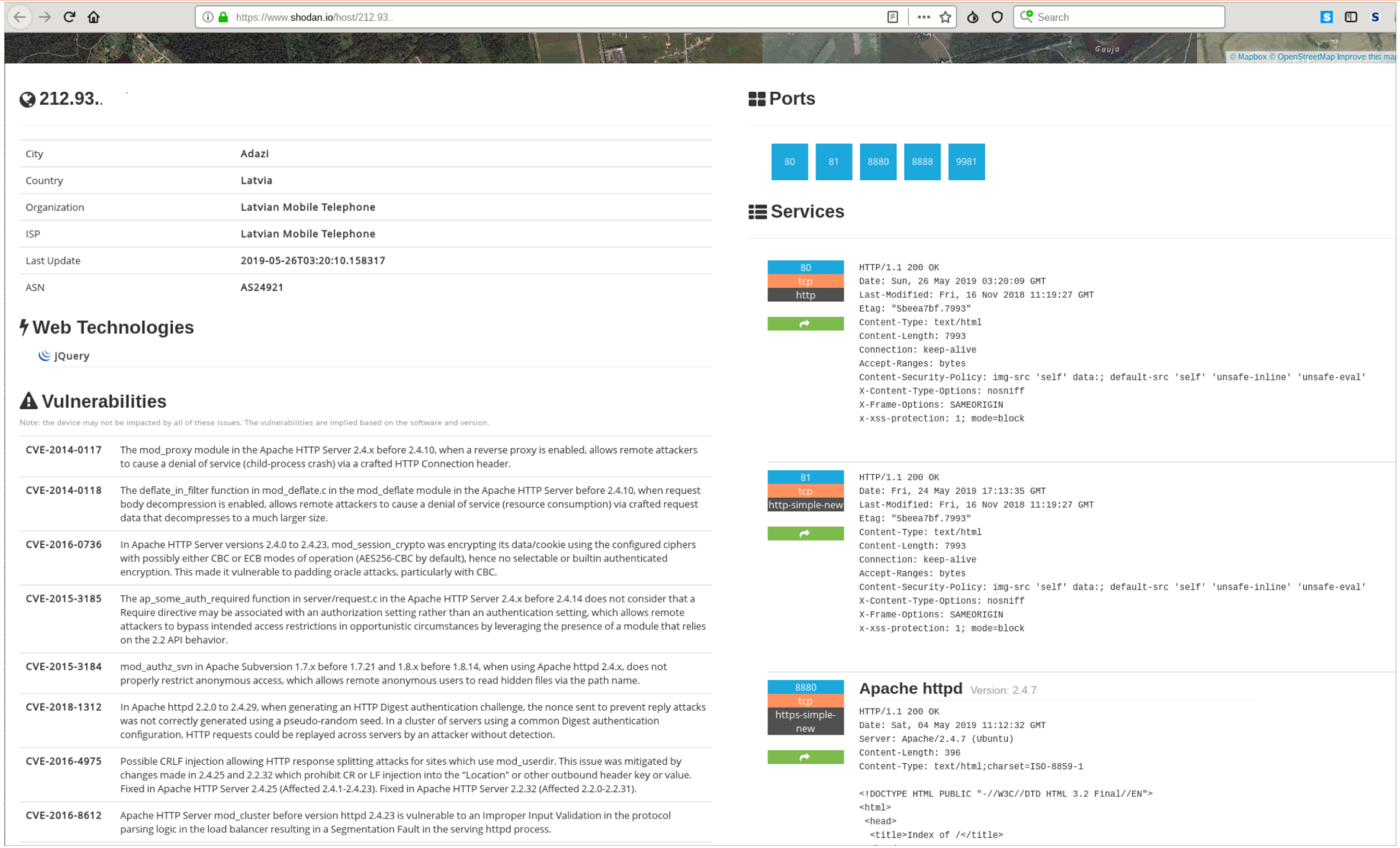
- **Pēc iekārtas uzstādīšanas tā netiek atjaunināta**
- **Lietotāji pat nezina, ko īsti pieslēguši internetam!**

Biežāka inficētās -IOT – aizmirstās iekārtas

- Pēc iekārtas uzstādīšanas tā netiek atjaunināta
- Lietotāji pat nezina, ko īsti pieslēguši internetam!
  - ✓Videonovērošanas sistēmas


NVR301-04LB-P4
212.93.
Search
Please click here to download and install the latest plug-in. Close your browser before installation.
unv
Username
Password
Login
Reset
1440*900 is recommended for best image quality.

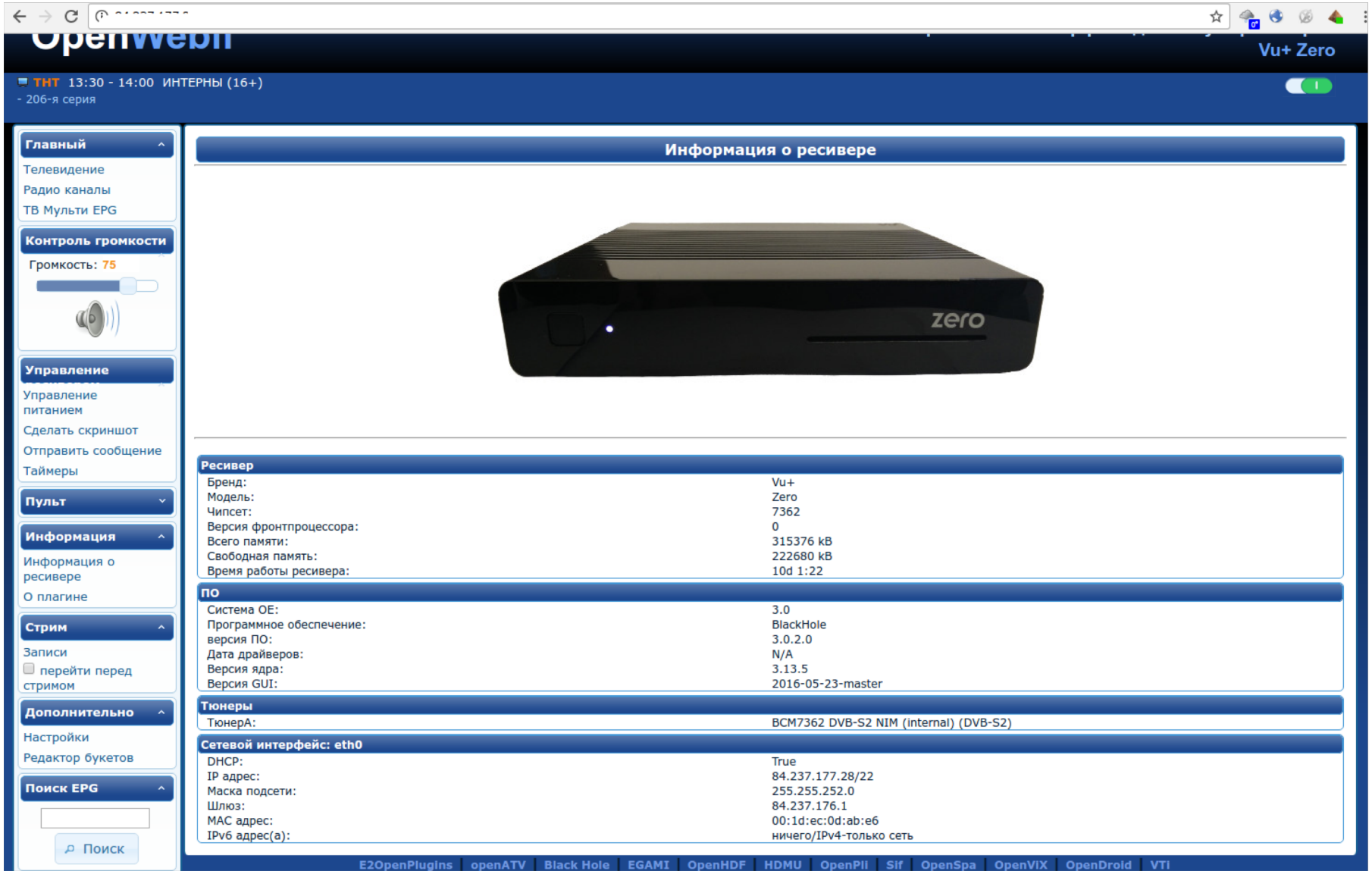

Saraksts ir tukšs
Jūsu grozs ir tukšs
Latviešu | English
Русский
LOKS
APSARDZES SISTĒMAS
Galvenā | Produkti | Lejupielādes | Ziņas | Par kompāniju
Meklēt
Katalogs
Videonovērošanas Sistēmas
UNIVIEW IP Sistēmas
IP Bullet Kameras
IP Bullet Smart Kameras
IP Kupola Kameras
IP Kupola Smart Kameras
IP Fisheye Kameras
IP PTZ Kameras
Videoreģistrātori NVR
Auto Numura Zīmes Atpazīšana
WiFi Komplekti
VMS Server
Sejas atpazīšana
Enkoderi & Dekoderi
Uniview Piederumi
PROVISION IP Sistēmas
DAHUA IP Sistēmas
HIKVISION IP Sistēmas
Wi-Fi IP Kameras
Mednieku Kameras
Bezvadu IP Sistēmas
AHD/TurboHD/TVI/CVI Sistēmas
Videonovērošanas Komplekti
Piederumi
Videonovērošanas Sistēmas Programmatūra
Tīkla Produkti
Apsardzes Sistēmas
Videonovērošanas ... | UNIVIEW IP Sistēmas | Videoreģistrātori NVR
Cena : bez PVN ar PVN
Videoreģistrātori NVR
NVR301-04LB-P4 ~ 2MPix IP NVR 4 kanāli/4PoE 40/40Mbps Ultra265 HDDx1
Kods: 008248
Pieejams: Jā
Cena: 94.50 EUR
Drukāt
Eksportēt
Sūtīt uz e-pastu
Instrukcija
Ielikt grozā
Apraksts
Specifikācija
Informācija
Lejupielādes
Video ieejas un izejas
4 ieejas (4 PoE) / HDMI x 1, VGA x 1
Audio ieejas un izejas
-
Video kompresija
Ultra265 / H.265 / H.264
Datu plūsma IN / OUT
40 / 40 Mbit
Maksimāla dekodēšana


https://www.shodan.io/host/212.93..
Search
Gauja
© Mapbox © OpenStreetMap Improve this map
212.93..
City Adazi
Country Latvia
Organization Latvian Mobile Telephone
ISP Latvian Mobile Telephone
Last Update 2019-05-26T03:20:10.158317
ASN AS24921
Web Technologies
jQuery
Vulnerabilities
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.
CVE-2014-0117 The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.
CVE-2014-0118 The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.
CVE-2016-0736 In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.
CVE-2015-3185 The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.
CVE-2015-3184 mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.
CVE-2018-1312 In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
CVE-2016-4975 Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).
CVE-2016-8612 Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.
Ports
80 81 8880 8888 9981
Services
80 tcp http
HTTP/1.1 200 OK
Date: Sun, 26 May 2019 03:20:09 GMT
Last-Modified: Fri, 16 Nov 2018 11:19:27 GMT
Etag: "5beea7bf.7993"
Content-Type: text/html
Content-Length: 7993
Connection: keep-alive
Accept-Ranges: bytes
Content-Security-Policy: img-src 'self' data:; default-src 'self' 'unsafe-inline' 'unsafe-eval'
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
x-xss-protection: 1; mode=block
81 tcp http-simple-new
HTTP/1.1 200 OK
Date: Fri, 24 May 2019 17:13:35 GMT
Last-Modified: Fri, 16 Nov 2018 11:19:27 GMT
Etag: "5beea7bf.7993"
Content-Type: text/html
Content-Length: 7993
Connection: keep-alive
Accept-Ranges: bytes
Content-Security-Policy: img-src 'self' data:; default-src 'self' 'unsafe-inline' 'unsafe-eval'
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
x-xss-protection: 1; mode=block
8880 tcp https-simple-new
Apache httpd Version: 2.4.7
HTTP/1.1 200 OK
Date: Sat, 04 May 2019 11:12:32 GMT
Server: Apache/2.4.7 (Ubuntu)
Content-Length: 396
Content-Type: text/html;charset=ISO-8859-1
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /</title>

Biežāka inficētās -IOT – aizmirstās iekārtas

- Pēc iekārtas uzstādīšanas tā netiek atjaunināta
- Lietotāji pat nezina, ko īsti pieslēguši internetam!
  - ✓Videonovērošanas sistēmas
  - ✓Satelītuztvērēji


OpenWebif
Открытый вэб интерфейс для линукс-ресиверов
Vu+ Zero
ТНТ 13:30 - 14:00 ИНТЕРНЫ (16+)
- 206-я серия
Главный
Телевидение
Радио каналы
ТВ Мульти EPG
Контроль громкости
Громкость: 75
Управление
Управление питанием
Сделать скриншот
Отправить сообщение
Таймеры
Пульт
Информация
Информация о ресивере
О плагине
Стрим
Записи
перейти перед стримом
Дополнительно
Настройки
Редактор букетов
Поиск EPG
Текущий
Букеты
Провайдеры
Спутники
Все каналы
EPG
HD
HTB+
Viasat
Latvija
Kino
Sport
Anime
Dokumental
Muzika
Novosti
XXX
Favourites (TV)

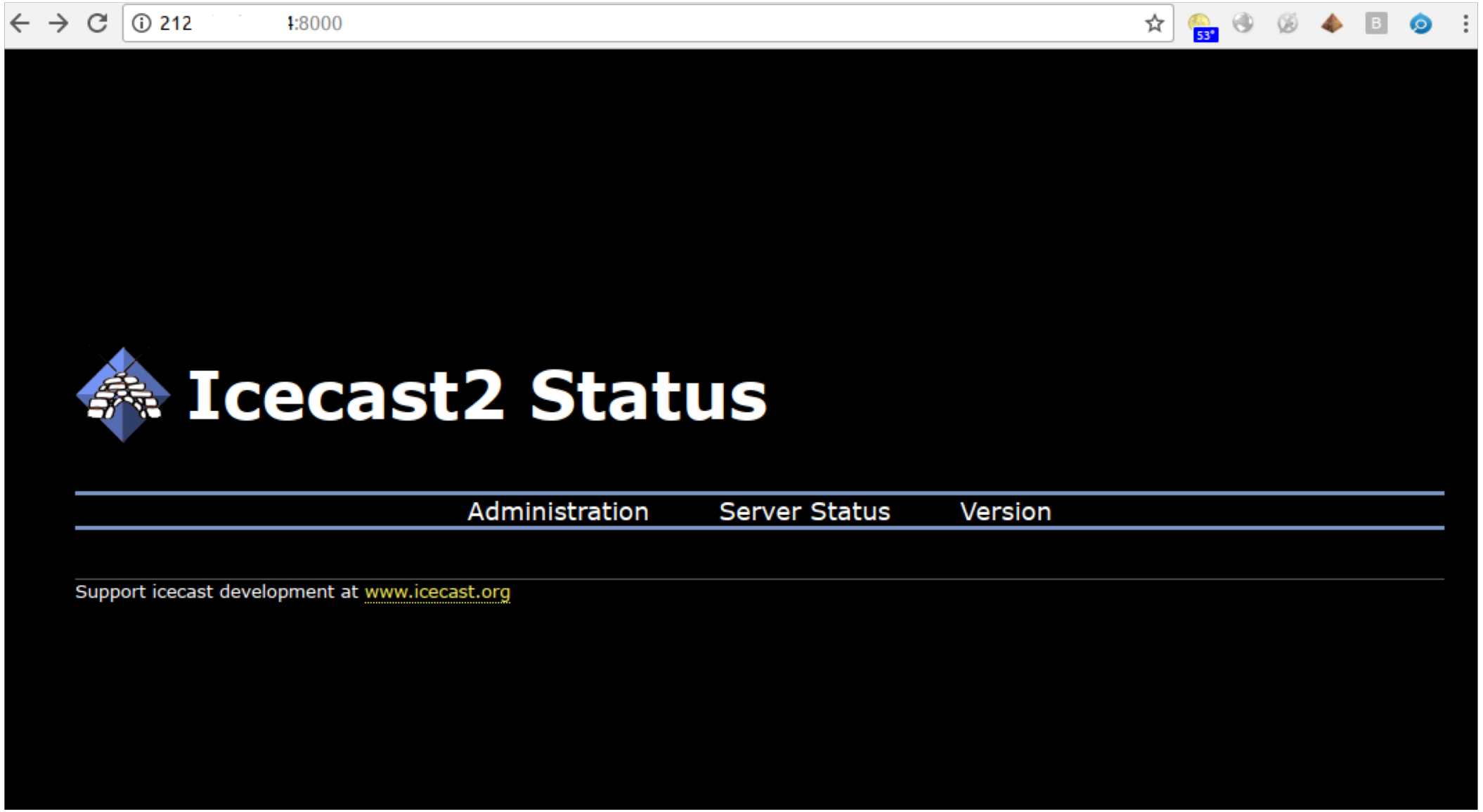

Vu+ Zero
ТНТ 13:30 - 14:00 ИНТЕРНЫ (16+)
- 206-я серия
Главный
Телевидение
Радио каналы
ТВ Мульти EPG
Контроль громкости
Громкость: 75
Управление
Управление питанием
Сделать скриншот
Отправить сообщение
Таймеры
Пульт
Информация
Информация о ресивере
О плагине
Стрим
Записи
перейти перед стримом
Дополнительно
Настройки
Редактор букетов
Поиск EPG
Поиск
Информация о ресивере
zero
Ресивер
Бренд: Vu+
Модель: Zero
Чипсет: 7362
Версия фронтпроцессора: 0
Всего памяти: 315376 kB
Свободная память: 222680 kB
Время работы ресивера: 10d 1:22
ПО
Система ОЕ: 3.0
Программное обеспечение: BlackHole
версия ПО: 3.0.2.0
Дата драйверов: N/A
Версия ядра: 3.13.5
Версия GUI: 2016-05-23-master
Тюнеры
ТюнерА: BCM7362 DVB-S2 NIM (internal) (DVB-S2)
Сетевой интерфейс: eth0
DHCP: True
IP адрес: 84.237.177.28/22
Маска подсети: 255.255.252.0
Шлюз: 84.237.176.1
MAC адрес: 00:1d:ec:0d:ab:e6
IPv6 адрес(а): ничего/IPv4-только сеть
E2OpenPlugins | openATV | Black Hole | EGAMI | OpenHDF | HDMU | OpenPli | Sif | OpenSpa | OpenViX | OpenDroid | VTi

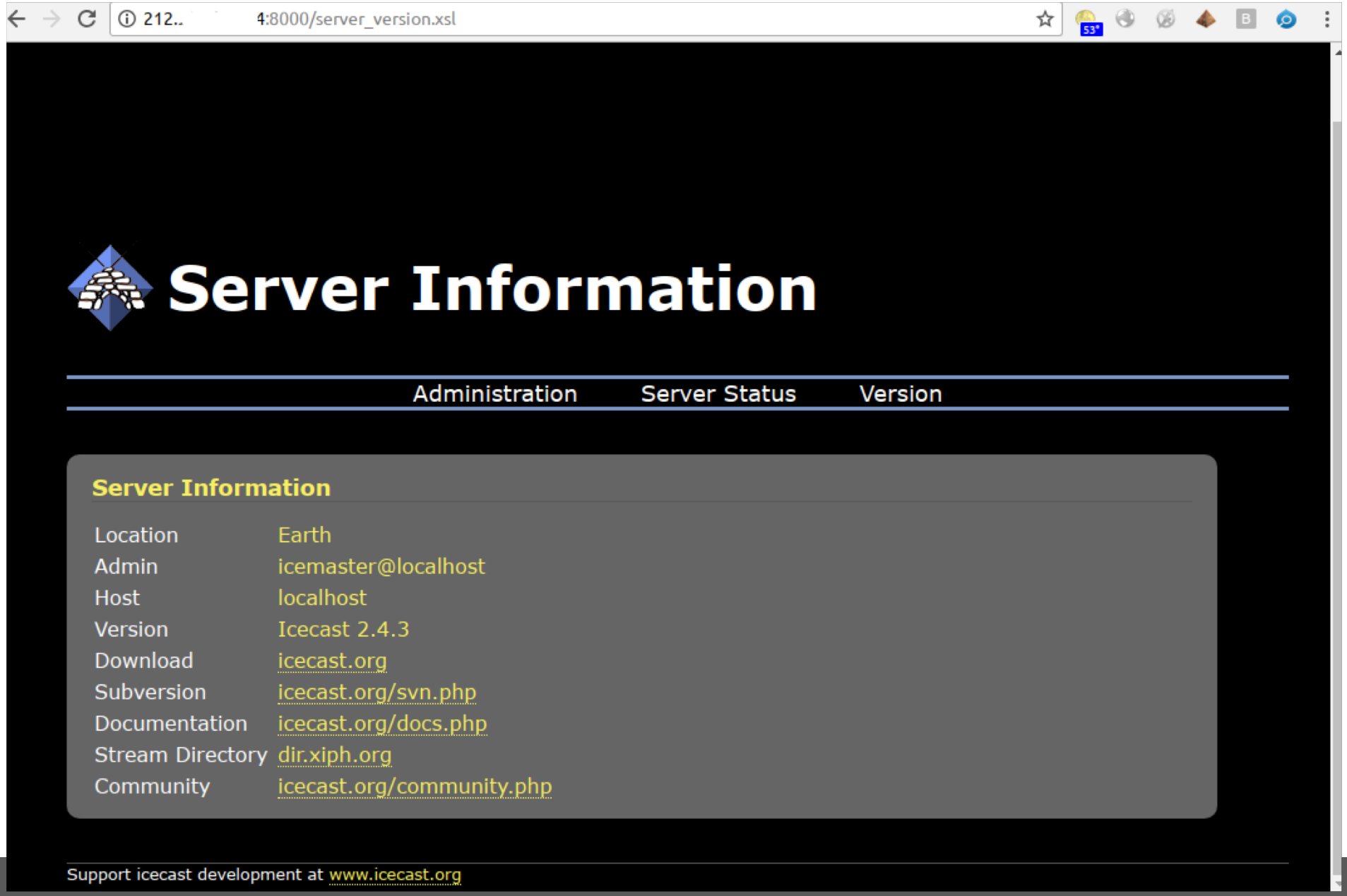
Biežāka inficētās -IOT – aizmirstās iekārtas

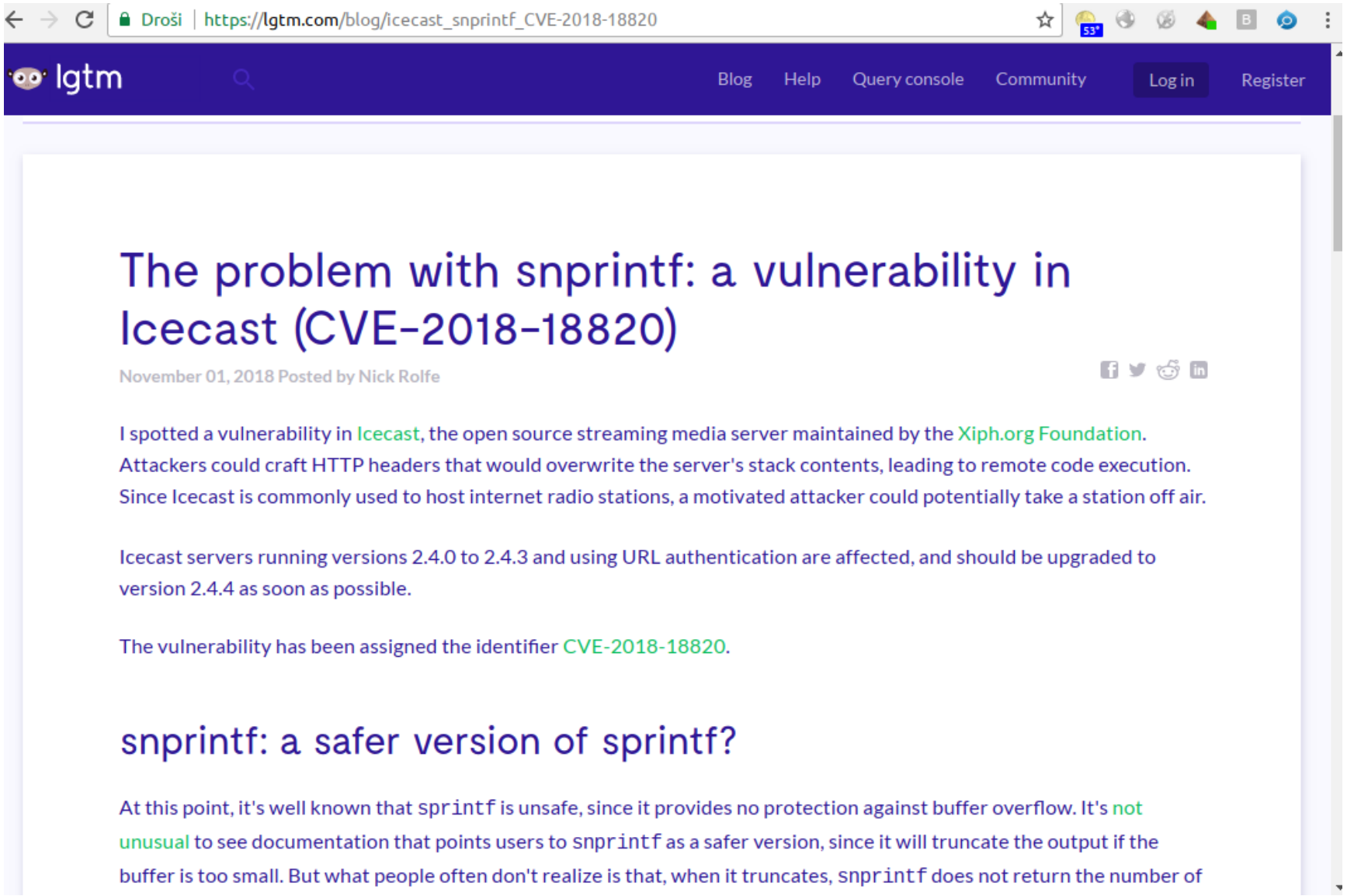
- Pēc iekārtas uzstādīšanas tā netiek atjaunināta
- Lietotāji pat nezina, ko īsti pieslēguši internetam!
  - ✓Videonovērošanas sistēmas
  - ✓Satelītuztvērēji
  - ✓Tīkla datu glabātavas

Biežāka inficētās -IOT – aizmirstās iekārtas

- Pēc iekārtas uzstādīšanas tā netiek atjaunināta
- Lietotāji pat nezina, ko īsti pieslēguši internetam!
  - ✓Videonovērošanas sistēmas
  - ✓Satelītuztvērēji
  - ✓Tīkla datu glabātavas
  - ✓Multimedia servers


212 :8000
Icecast2 Status
Administration
Server Status
Version
Support icecast development at www.icecast.org


212..
4:8000/server_version.xsl
Server Information
Administration
Server Status
Version
Server Information
Location Earth
Admin icemaster@localhost
Host localhost
Version Icecast 2.4.3
Download icecast.org
Subversion icecast.org/svn.php
Documentation icecast.org/docs.php
Stream Directory dir.xiph.org
Community icecast.org/community.php
Support icecast development at www.icecast.org



Droši | https://lgtm.com/blog/icecast_snprintf_CVE-2018-18820

lgtm

Blog Help Query console Community Log in Register

The problem with snprintf: a vulnerability in Icecast (CVE-2018-18820)

November 01, 2018 Posted by Nick Rolfe

I spotted a vulnerability in Icecast, the open source streaming media server maintained by the Xiph.org Foundation. Attackers could craft HTTP headers that would overwrite the server's stack contents, leading to remote code execution. Since Icecast is commonly used to host internet radio stations, a motivated attacker could potentially take a station off air.

Icecast servers running versions 2.4.0 to 2.4.3 and using URL authentication are affected, and should be upgraded to version 2.4.4 as soon as possible.

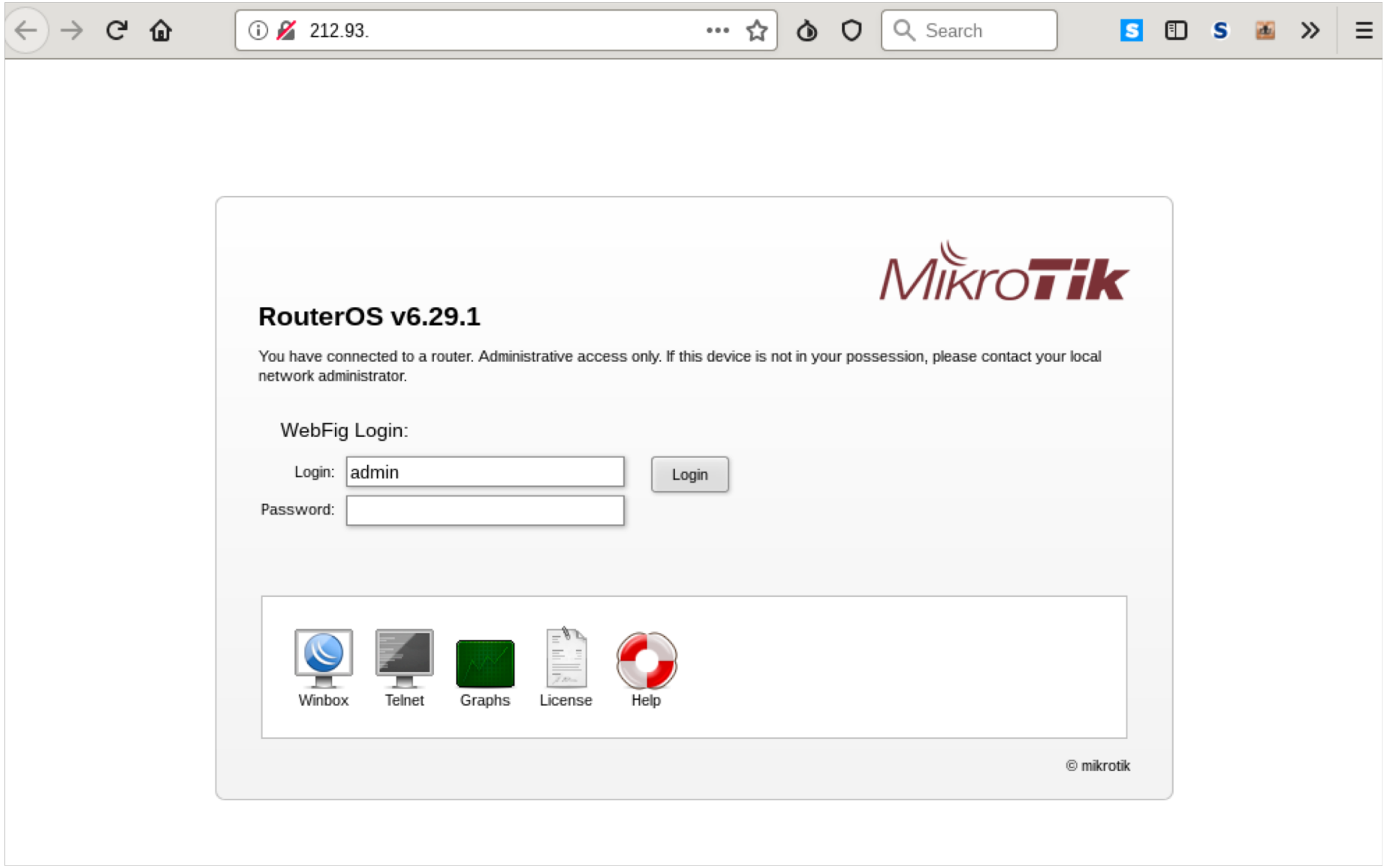
The vulnerability has been assigned the identifier CVE-2018-18820.

snprintf: a safer version of sprintf?

At this point, it's well known that `sprintf` is unsafe, since it provides no protection against buffer overflow. It's not unusual to see documentation that points users to `snprintf` as a safer version, since it will truncate the output if the buffer is too small. But what people often don't realize is that, when it truncates, `snprintf` does not return the number of

Biežāka inficētās -IOT – aizmirstās iekārtas

- Pēc iekārtas uzstādīšanas tā netiek atjaunināta
- Lietotāji pat nezina, ko īsti pieslēguši internetam!
  - ✓Videonovērošanas sistēmas
  - ✓Satelītuztvērēji
  - ✓Tīkla datu glabātavas
  - ✓Multimedia servers
  - ✓Maršrutētāji


212.93.
Search
MikroTik
RouterOS v6.29.1
You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.
WebFig Login:
Login: admin
Login
Password:
Winbox
Telnet
Graphs
License
Help
© mikrotik

Mikrotik » Routeros : Security Vulnerabilities Published In 2018

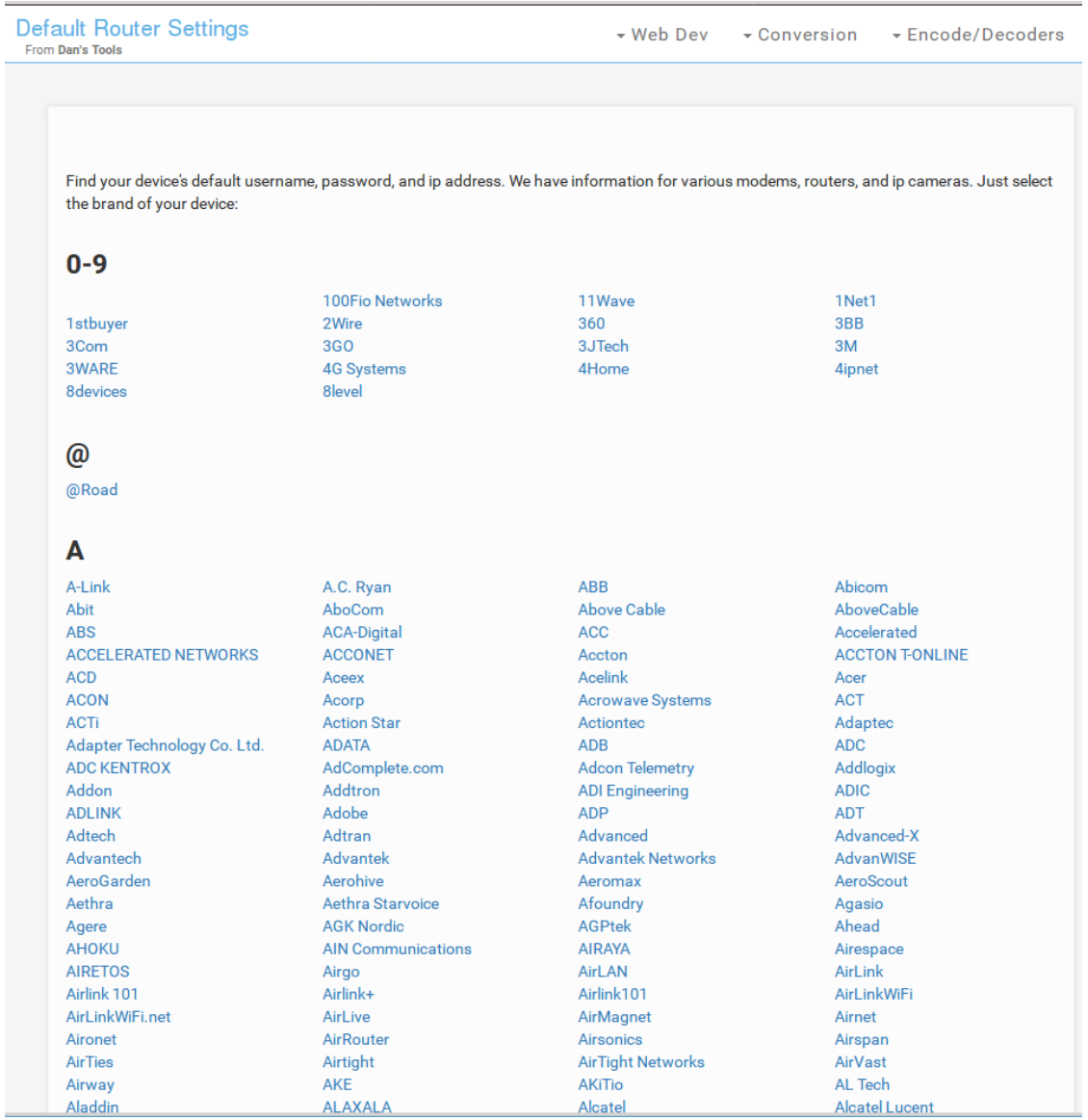
2018 : January February March April May June July August September October November December CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication
1	CVE-2018-14847	287		Dir. Trav.	2018-08-02	2018-11-16	5.0	None	Remote	Low	Not required
MikroTik RouterOS through 6.42 allows unauthenticated remote attackers to read arbitrary files and remote authenticated attackers to write arbitrary files due to a directory traversa interface.											
2	CVE-2018-7445	119		Exec Code Overflow	2018-03-19	2018-04-24	10.0	None	Remote	Low	Not required
A buffer overflow was found in the MikroTik RouterOS SMB service when processing NetBIOS session request messages. Remote attackers with access to the service can exploit this execution on the system. The overflow occurs before authentication takes place, so it is possible for an unauthenticated remote attacker to exploit it. All architectures and all devices 6.41.3/6.42rc27 are vulnerable.											
3	CVE-2018-1159	119		Overflow Mem. Corr.	2018-08-23	2018-10-12	4.0	None	Remote	Low	Single system
Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a memory corruption vulnerability. An authenticated remote attacker can crash the HTTP server by rapidly authenticating											
4	CVE-2018-1158	400			2018-08-23	2018-10-12	4.0	None	Remote	Low	Single system
Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a stack exhaustion vulnerability. An authenticated remote attacker can crash the HTTP server via recursive parsing of JS											
5	CVE-2018-1157	400			2018-08-23	2018-11-23	6.8	None	Remote	Low	Single system
Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a memory exhaustion vulnerability. An authenticated remote attacker can crash the HTTP server and in some circumstar HTTP POST request.											
6	CVE-2018-1156	119		Exec Code Overflow	2018-08-23	2018-11-23	9.0	None	Remote	Low	Single system
Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to stack buffer overflow through the license upgrade interface. This vulnerability could theoretically allow a remote authent code on the system.											

Total number of vulnerabilities : **6** Page : 1 (This Page)



Default Router Settings
From Dan's Tools

Web Dev | Conversion | Encode/Decoders

Find your device's default username, password, and ip address. We have information for various modems, routers, and ip cameras. Just select the brand of your device:

0-9

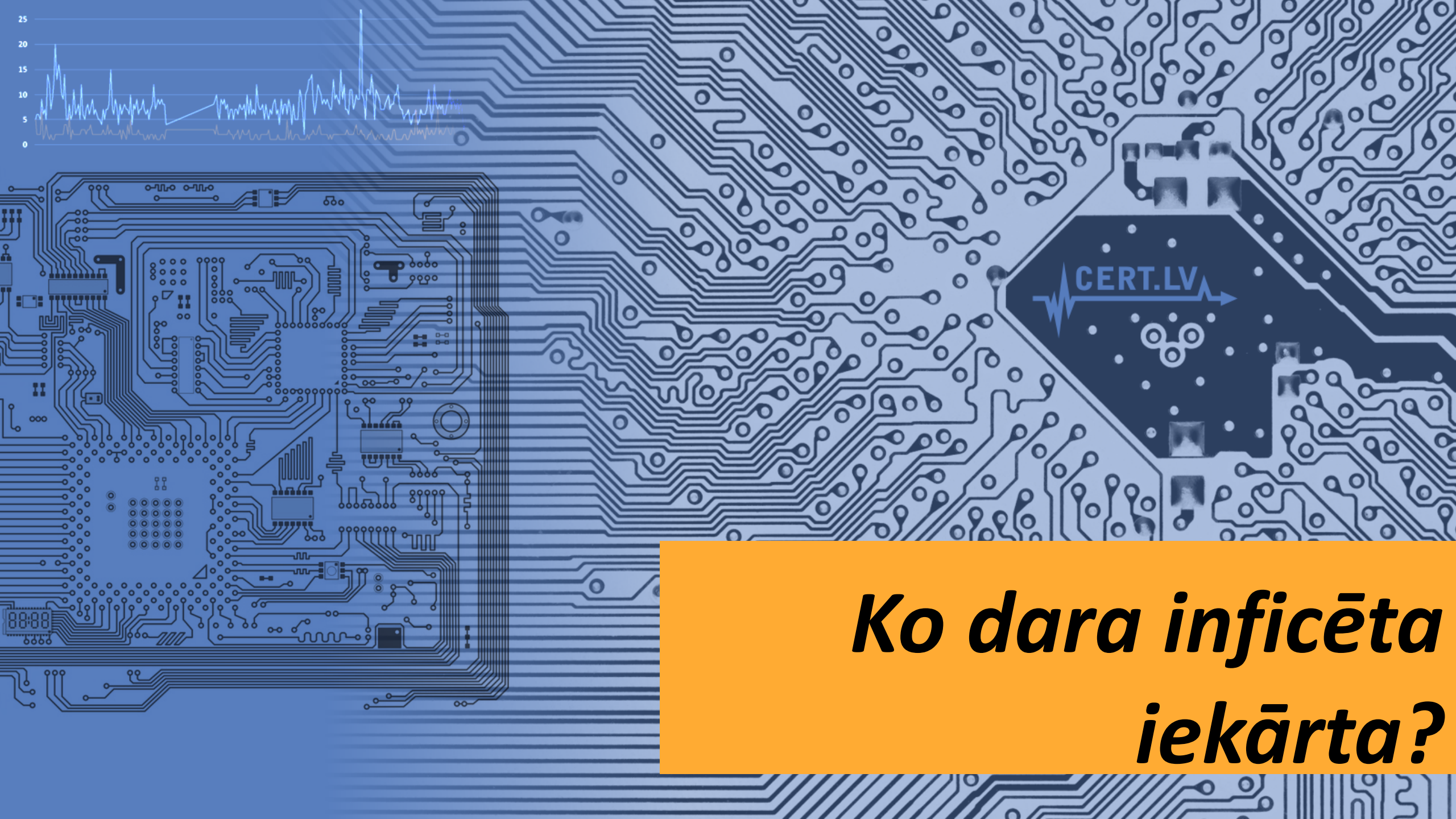
100Fio Networks
11Wave
1Net1
1stbuyer
2Wire
360
3BB
3Com
3GO
3JTech
3M
3WARE
4G Systems
4Home
4ipnet
8devices
8level

@

@Road

A

A-Link
A.C. Ryan
ABB
Abicom
Abit
AboCom
Above Cable
AboveCable
ABS
ACA-Digital
ACC
Accelerated
ACCELERATED NETWORKS
ACCONET
Accton
ACCTON T-ONLINE
ACD
Aceex
Acelink
Acer
ACON
Acorp
Acrowave Systems
ACT
ACTi
Action Star
Actiontec
Adaptec
Adapter Technology Co. Ltd.
ADATA
ADB
ADC
ADC KENTROX
AdComplete.com
Adcon Telemetry
Addlogix
Addon
Addtron
ADI Engineering
ADIC
ADLINK
Adobe
ADP
ADT
Adtech
Adtran
Advanced
Advanced-X
Advantech
Advantek
Advantek Networks
AdvanWISE
AeroGarden
Aerohive
Aeromax
AeroScout
Aethra
Aethra Starvoice
Afoundry
Agasio
Agere
AGK Nordic
AGPtek
Ahead
AHOKU
AIN Communications
AIRAYA
Airespace
AIRETOS
Airgo
AirLAN
AirLink
Airlink 101
Airlink+
Airlink101
AirLinkWiFi
AirLinkWiFi.net
AirLive
AirMagnet
Airnet
Aironet
AirRouter
Airsonics
Airspan
AirTies
Airtight
AirTight Networks
AirVast
Airway
AKE
AKiTio
AL Tech
Aladdin
ALAXALA
Alcatel
Alcatel Lucent



Ko dara inficēta iekārta?

1. Neparastas darbības datortīklā

- Ievainojamību meklēšana apkārtējos datortīkla segmentos
- Palielināts SMPT trafiks (mēstules)
- Mēģinajumi minēt POP3/IMAP paroles
- Masveida RDP pieslēgumu mēģinājumi

2. Neraksturīgi servisi

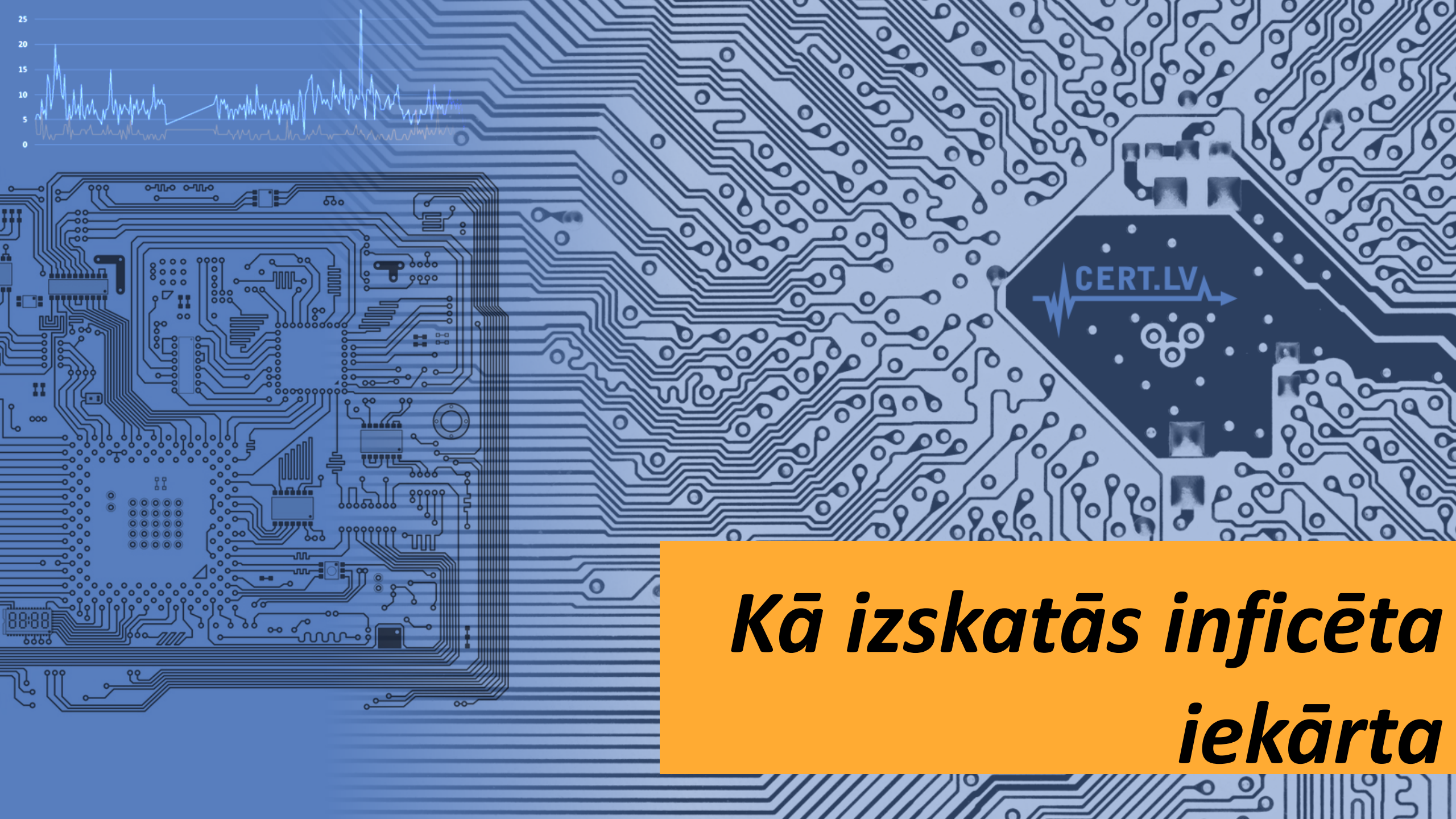
- Aktīvi HTTP/Socks Proxy
- Open Relay SMTP
- Open DNS resolver
- Pieejams RDP uz nestandarta portiem
- Aktīvi VPN servisi

3. Neparasta datu plūsma

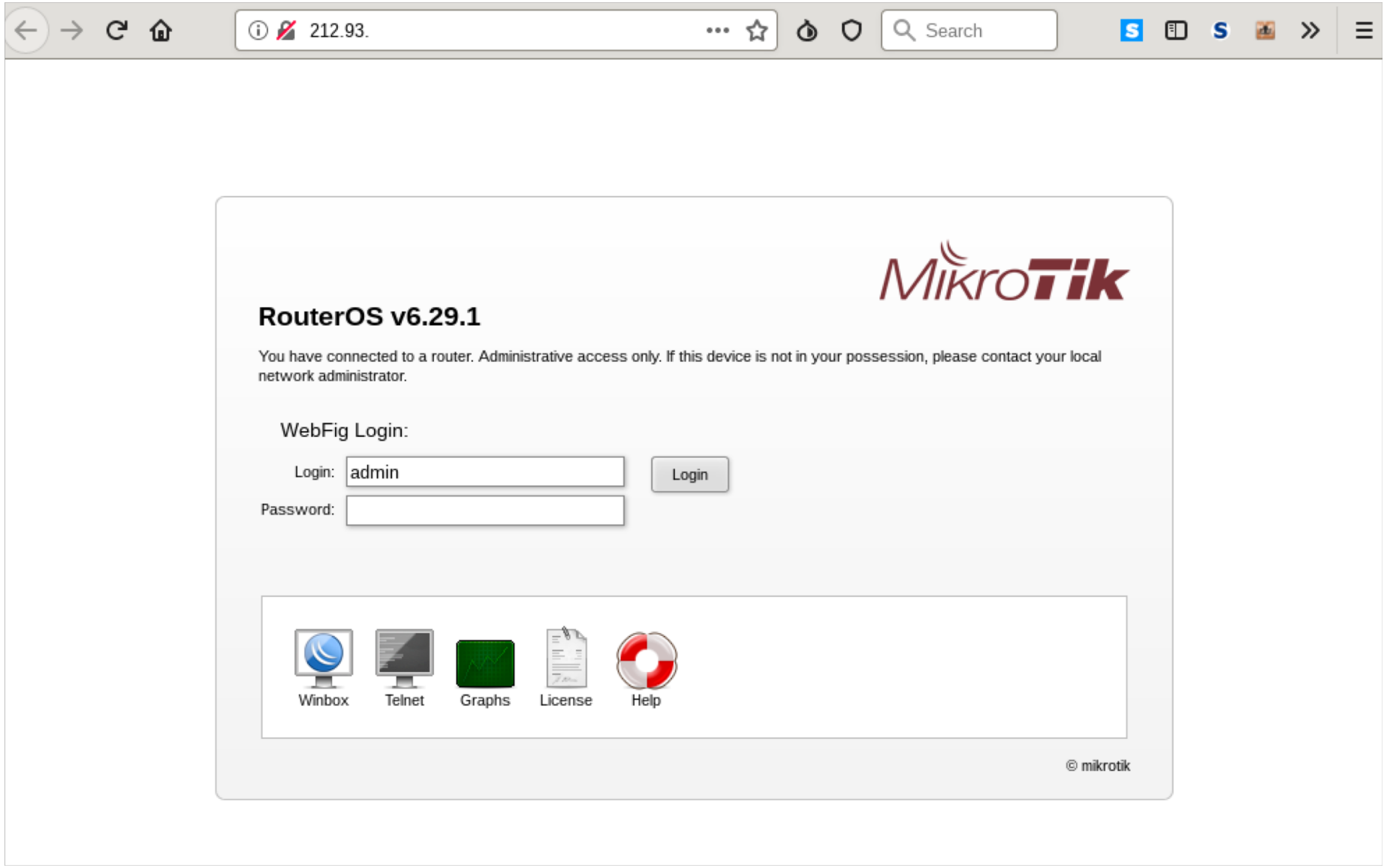
- Palielināts SSH, Telnet trafiks
- IPV6 trafiks ar nezināmu izcelsmi
- Liela izejošo UDP datu plūsma

4. Atvērti vārti uz iekšējo tīklu

- Iespējams piekļūt nepubliskiem tīkla segmentiem, apiet uz IP adresēm balstītus ierobežojumus
- Datu plūsmas pārtveršana, piekļuve nešifrēti pārraidītām parolēm (POP3, IMAP, FTP, Syslog utt.)
- Windows domēnu autentifikācijas pārtveršana (kerberos golden ticket, pass-the-hash utt.)



Kā izskatās inficēta iekārta


212.93.
Search
MikroTik
RouterOS v6.29.1
You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.
WebFig Login:
Login: admin
Login
Password:
Winbox
Telnet
Graphs
License
Help
© mikrotik


rying 212.
Connected to 212.3
Escape character is '^]'.
login: admin
Password:
Another cli session is active
Do you wish to continue? [y/N] y
admin@geneko>
admin@geneko>
admin@geneko>
admin@geneko>

Device configuration using web application

The GWR-HS Router's web–based utility allows you to set up the Router and perform advanced configuration and troubleshooting. This chapter will explain all of the functions in this utility.

For local access to the GWR-HS Router's web–based utility, launch your web browser, and enter the Router's default IP address, 192.168.1.1, in the address field. A login screen prompts you for your User name and Password. Default administration credentials are admin/admin.

If you want to use web interface for router administration please enter IP address of router into web browser. Please disable Proxy server in web browser before proceed.

ManualsLib.com

Figure 8 – User authentication

After successfully finished process of authentication of Username/Password you can access Main Configuration *Menu.*

You can set all parameters of the GWR-HS Router using web application. All functionalities and parameters are organized within few main tabs (windows).

Uzlauzts maršrutrētājs

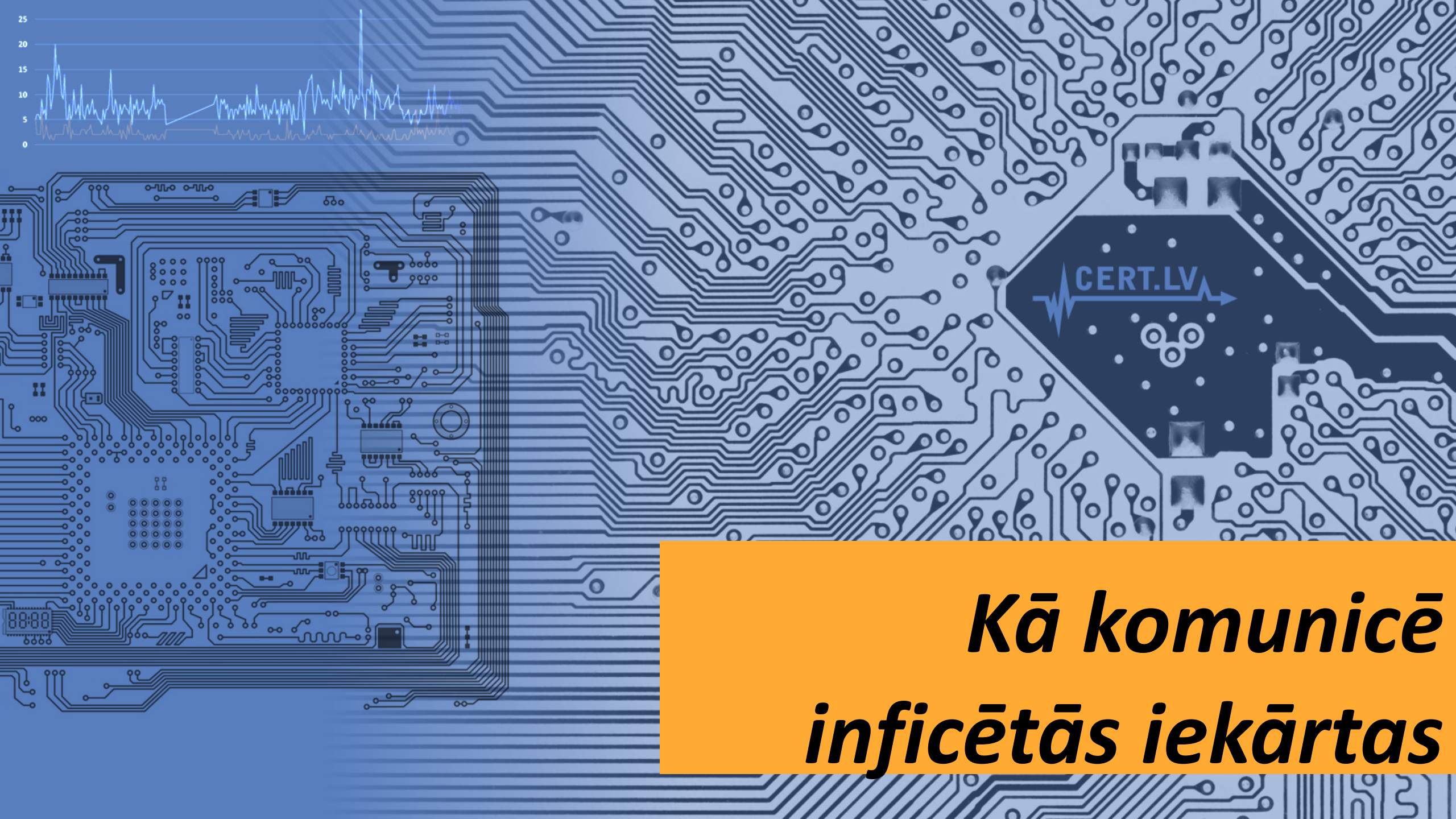
```
1  $ nmap 212.93.
2
3  Starting Nmap 6.40 ( http://nmap.org ) at 2019-05-29 14:11 EEST
4  Nmap scan report for 212.93.
5  Host is up (0.032s latency).
6  Not shown: 993 closed ports
7  PORT     STATE SERVICE
8  21/tcp   open  ftp
9  22/tcp   open  ssh
10 23/tcp   open  telnet
11 80/tcp   open  http
12 1723/tcp open  pptp
13 2000/tcp open  cisco-sccp
14 8291/tcp open  unknown
15
16 Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds
```

Uzlauzts maršrutrētājs

```
$ nmap 212.93.

Starting Nmap 6.40 ( http://nmap.org ) at 2019-05-29 14:54 EEST
Nmap scan report for 212.93.
Host is up (0.036s latency).
Not shown: 992 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
53/tcp   open     domain
80/tcp   open     http
1723/tcp open     pptp
2000/tcp open     cisco-sccp
3389/tcp open     ms-wbt-server
8081/tcp open     blackice-icecap
8291/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
```

C&C serveris

```
$ nmap 5.188.

Starting Nmap 6.40 ( http://nmap.org ) at 2019-05-31 13:15 EEST
Nmap scan report for hostby.chan
Host is up (0.068s latency).
Not shown: 928 closed ports
PORT      STATE    SERVICE
25/tcp    filtered smtp
111/tcp   open     rpcbind
3389/tcp  open     ms-wbt-server
10000/tcp open     snet-sensor-mgmt
10001/tcp open     scp-config
10002/tcp open     documentum
10003/tcp open     documentum_s
10004/tcp open     emcrmirccd
10009/tcp open     swdtp-sv
10010/tcp open     rxapi
10012/tcp open     unknown
10024/tcp open     unknown
10025/tcp open     unknown
10082/tcp open     amandaidx
10180/tcp open     unknown
10215/tcp open     unknown
10243/tcp open     unknown
10566/tcp open     unknown
10616/tcp open     unknown
10617/tcp open     unknown
10621/tcp open     unknown
10626/tcp open     unknown
10628/tcp open     unknown
```

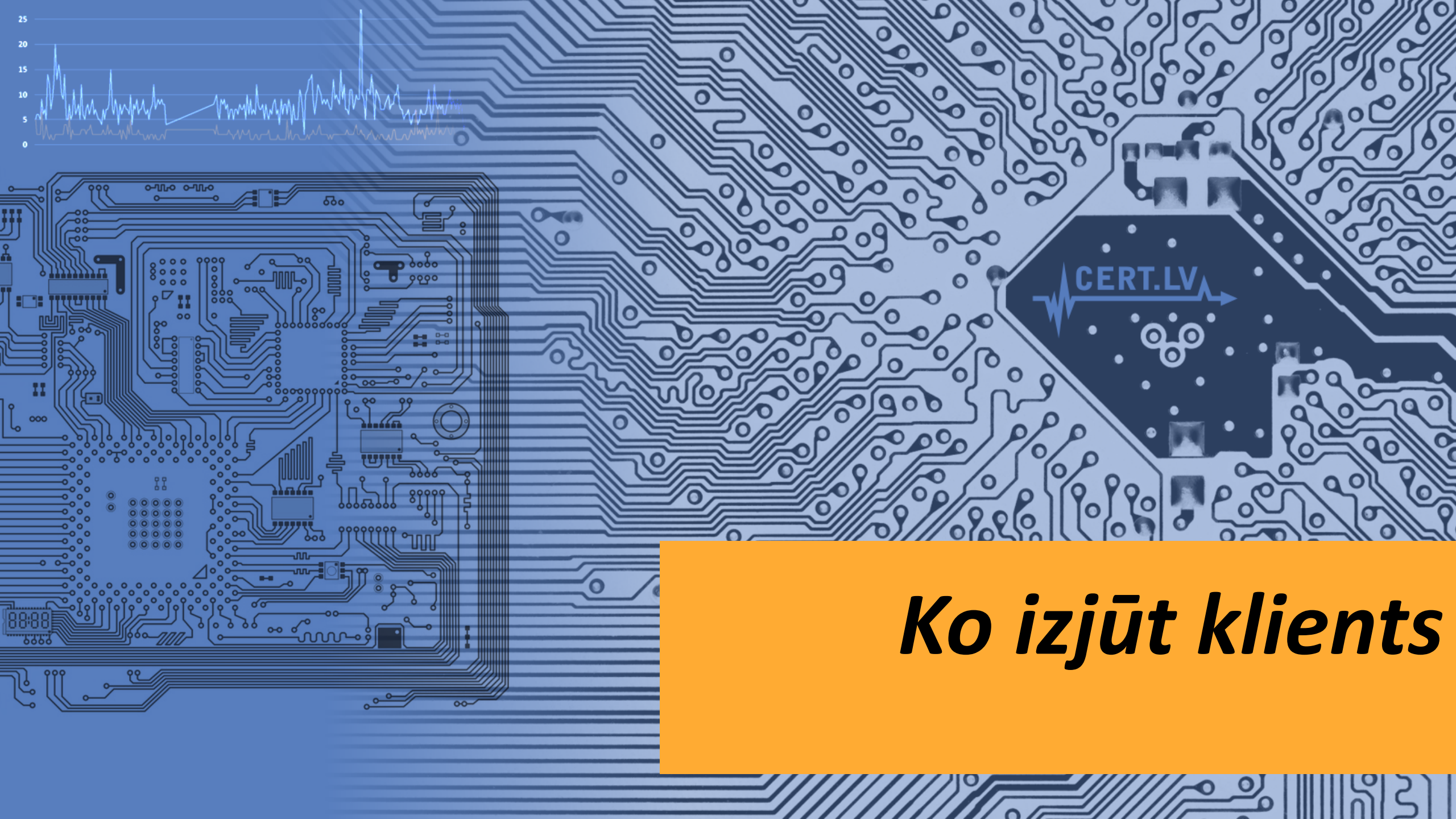


Kā komunicē inficētās iekārtas

Komunikācijas tipi

- P2P saziņa – Telnet, SSH, HTTP
- Saziņa ar C&C – HTTP, FTP, Remote dektop, SSH
- IPV6 datu plūsma, izmantojot standarta protokolus

```
206 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.175.209:60089 TIME_WAIT   -
207 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.169.25:55325 TIME_WAIT   -
208 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.167.35:37762 TIME_WAIT   -
209 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.167.35:37718 TIME_WAIT   -
210 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.169.25:55002 TIME_WAIT   -
211 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.169.25:55150 TIME_WAIT   -
212 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.175.209:60117 TIME_WAIT   -
213 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.175.209:60124 TIME_WAIT   -
214 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:189.110.130.156:39542 TIME_WAIT   -
215 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:189.110.130.156:39545 TIME_WAIT   -
216 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.169.25:55249 TIME_WAIT   -
217 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.167.35:38166 ESTABLISHED -
218 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.175.209:59939 TIME_WAIT   -
219 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.175.209:59764 TIME_WAIT   -
220 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.167.35:38023 TIME_WAIT   -
221 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.169.25:55170 TIME_WAIT   -
222 tcp        0     20 ::ffff:212.3.*.*:23 ::ffff:189.110.130.156:39549 FIN_WAIT1   -
223 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.175.209:60002 TIME_WAIT   -
224 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.167.35:38068 TIME_WAIT   -
225 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.167.35:37888 TIME_WAIT   -
226 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.175.209:59871 TIME_WAIT   -
227 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.169.25:55079 TIME_WAIT   -
228 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.169.25:55224 TIME_WAIT   -
229 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.167.35:38063 TIME_WAIT   -
230 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.175.209:59841 TIME_WAIT   -
231 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:189.110.130.156:39547 TIME_WAIT   -
232 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.167.35:37916 TIME_WAIT   -
233 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.175.209:59919 TIME_WAIT   -
234 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.169.25:55350 ESTABLISHED -
235 tcp        0      2 ::ffff:212.3.*.*:23 ::ffff:212.3.175.209:60135 ESTABLISHED -
236 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.169.25:55293 TIME_WAIT   -
237 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:189.110.130.156:39544 TIME_WAIT   -
238 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.167.35:37876 TIME_WAIT   -
239 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.167.35:37739 TIME_WAIT   -
240 tcp        0      0 ::ffff:212.3.*.*:23 ::ffff:212.3.175.209:59904 TIME_WAIT   -
241
```



Ko izjūt klients

CERT.LV

```
tcp        0      0 212.3.*.*:22            62.112.11.79:47798      ESTABLISHED -
tcp        0      0 212.3.*.*:22            5.188.86.209:54243      ESTABLISHED -
tcp        0      0 212.3.*.*:35573         35.186.213.138:443      CLOSE_WAIT  -
tcp        0      0 212.3.*.*:35523         35.186.213.138:443      CLOSE_WAIT  -
tcp        0      0 212.3.*.*:57534         213.180.147.146:25      TIME_WAIT   -
tcp        0      0 212.3.*.*:37175         87.250.250.242:80       TIME_WAIT   -
tcp        0      0 212.3.*.*:46642         64.233.165.108:993      CLOSE_WAIT  -
tcp        0      0 212.3.*.*:42771         184.86.7.86:443         ESTABLISHED -
tcp        0      0 212.3.*.*:60431         212.93.97.104:80        ESTABLISHED -
tcp        0      1 212.3.*.*:47860         222.181.93.130:22       SYN_SENT    -
tcp        0      0 212.3.*.*:22            185.220.221.222:65072   ESTABLISHED -
tcp        0      0 212.3.*.*:22            62.112.11.223:7950      ESTABLISHED -
tcp        0      0 212.3.*.*:22            62.112.11.9:45462       ESTABLISHED -
tcp        0      0 212.3.*.*:44100         205.185.208.142:443     CLOSE_WAIT  -
tcp        0      0 212.3.*.*:22            5.188.86.167:33970      ESTABLISHED -
tcp        0      0 212.3.*.*:44010         184.86.7.86:443         CLOSE_WAIT  -
tcp        0      0 212.3.*.*:22            62.112.11.222:9176      ESTABLISHED -
tcp        0      0 212.3.*.*:22            5.188.87.54:49426       ESTABLISHED -
tcp        0      0 212.3.*.*:22            5.188.86.202:60768      ESTABLISHED -
tcp        0      0 212.3.*.*:22            185.248.103.136:35069   ESTABLISHED -
tcp        0      0 212.3.*.*:37169         87.250.250.242:80       TIME_WAIT   -
tcp        0      1 212.3.*.*:55337         123.158.8.190:22        SYN_SENT    -
tcp        0      1 212.3.*.*:44932         23.61.214.64:443        FIN_WAIT1   -
tcp        0      0 212.3.*.*:50324         31.13.72.53:443         CLOSE_WAIT  -
tcp        0      0 212.3.*.*:35798         35.186.213.138:443      CLOSE_WAIT  -
tcp        0      0 212.3.*.*:35861         35.186.213.138:443      CLOSE_WAIT  -
tcp        0      1 212.3.*.*:33843         188.62.8.13:22          SYN_SENT    -
tcp        0      0 212.3.*.*:22            185.248.103.178:62958   ESTABLISHED -
tcp        0      0 212.3.*.*:22            212.8.248.194:55148     ESTABLISHED -
tcp        0      0 212.3.*.*:58328         212.93.97.104:443       TIME_WAIT   -
```

Šifrējošie izspiedējvīrusi - ielaušanās

Uzņēmumi nepietiekmi kontrolē attālinātu piekļuvi saviem datiem

- RDP piekļuve sensitīvajiem datiem (NE GDPR izpratnē!) – grāmatvedībai un noliktavām
- Bez vajadzības uzstādīti TeamViewer utt. rīki
- Netiek izmantota NEKĀDA attālināta pieslēguma aizsardzība (VPN utt.)
- Netiek veikta piekļuves mēģinājumu auditēšana un kontrole
- Parole nav pietiekami droša
- Piekļuve tīklā nodrošina pārāk lielas tiesības tajā
- RDP uz nestandarta porta nepalielina drošību!

Šifrējošie izspiedējvīrusi - ielaušanās

Taisiet REZERVES KOPIJAS!!

- Atkopšanās no šifrējošajiem datorvīrusiem var prasīt mēnešus
- Finansiālie zaudējumi ir vairāki tūkstoši/desmiti tūkstši EUR
- Datus var izdoties neatgūt nekad – arī vīrusu autori kļūdās!
- Maksāšana izspiedējiem tikai veicina šos uzbrukumus
- Var tik skartas unikālas informācijas glabātavas
- Uzbrukums medicīnas iestādēm var kādam maksāt dzīvību vai veselību

Mēstulu izsūtīšana

Mēstuļu izsūtīšana var radīt ilglaicīgas sekas!

- Traucēta normāla e-pasta plūsma, pārslogoti serveri
- IP adreses nonākšana melnajos sarakstos
- «reputācijas» pasliktināšanās e-pasta apstrādes platformās
- Aizkavēta un «pazudusi» biznesa sarakste
- Apdraud visu IPS vai apakštīklu, daži filtri bloķē vismaz /24

DDOS amplifier

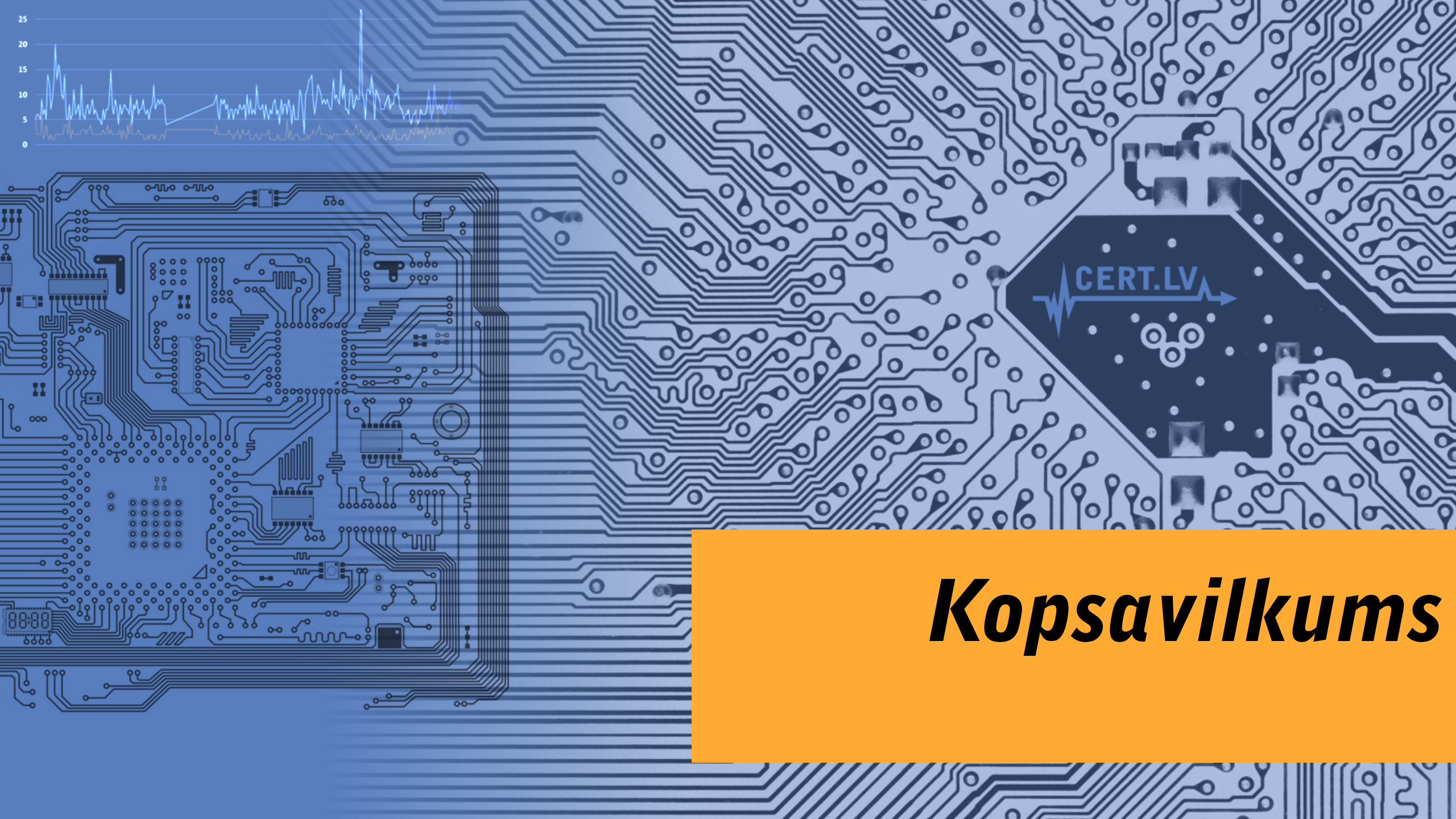
Pieejama iekārta var, un tiks iesaistīta DDOS uzbrukumos!

- Lai izmantotu iekārtu DOS uzbrukumiem tā nav «jāuzlauž»
- Ne visās iekārtās lietotājs var atslēgt problemātiskos servisus
- Kļūdas pievienojot jaunas iekārtas (LAN/WAN, ugunsmūris)
- DDOS uzbrukums var sākties pēkšņi un ievērojami pārslogot datortīklu
- Ja iekšējā tīklā ir daudz kompromitētu iekārtu nepietiks ar ienākošās datu plūsmas ierobežošanu!

Mikrotik Coinhive infekcija

- Izmanto Winbox ievainojamību (publiski zināma no 24.04.2018.)
- Izveido SOCKS proxy servisu, tam iespējams piekļūt arī no interneta
- Pievieno Coinhive kriptovalūtas ģenerācijas skriptu visām, vai arī tikai kļūdainajām interneta vietnēm, kas apmeklētas caur šo proxy
- Praktiski nemanāma maršrutētāja lietotājam
- Saglabājas arī pēc maršrutētāja programmnodrošinājuma atjaunināšanas, ja netiek apzināti noņemta
- Latvijā konstatēts ~1000 iekārtām

Pie SOCKS PROXY uzturētāja reāli var ierasties policija ar kratīšanas orderi!



Kopsavilkums

Tendences

- Šifrējošie vīrusi joprojām aktuāli
- RDP ir nopietns drauds
- DDoS atkal ir modē
- Dažāda veida krāpšanas un izspiešanas shēmas
- Maršrutizētāju ievainojamības
- IoT un mobilo iekārtu ļaunatūras daudzums palielinās

Paldies!

www.cert.lv