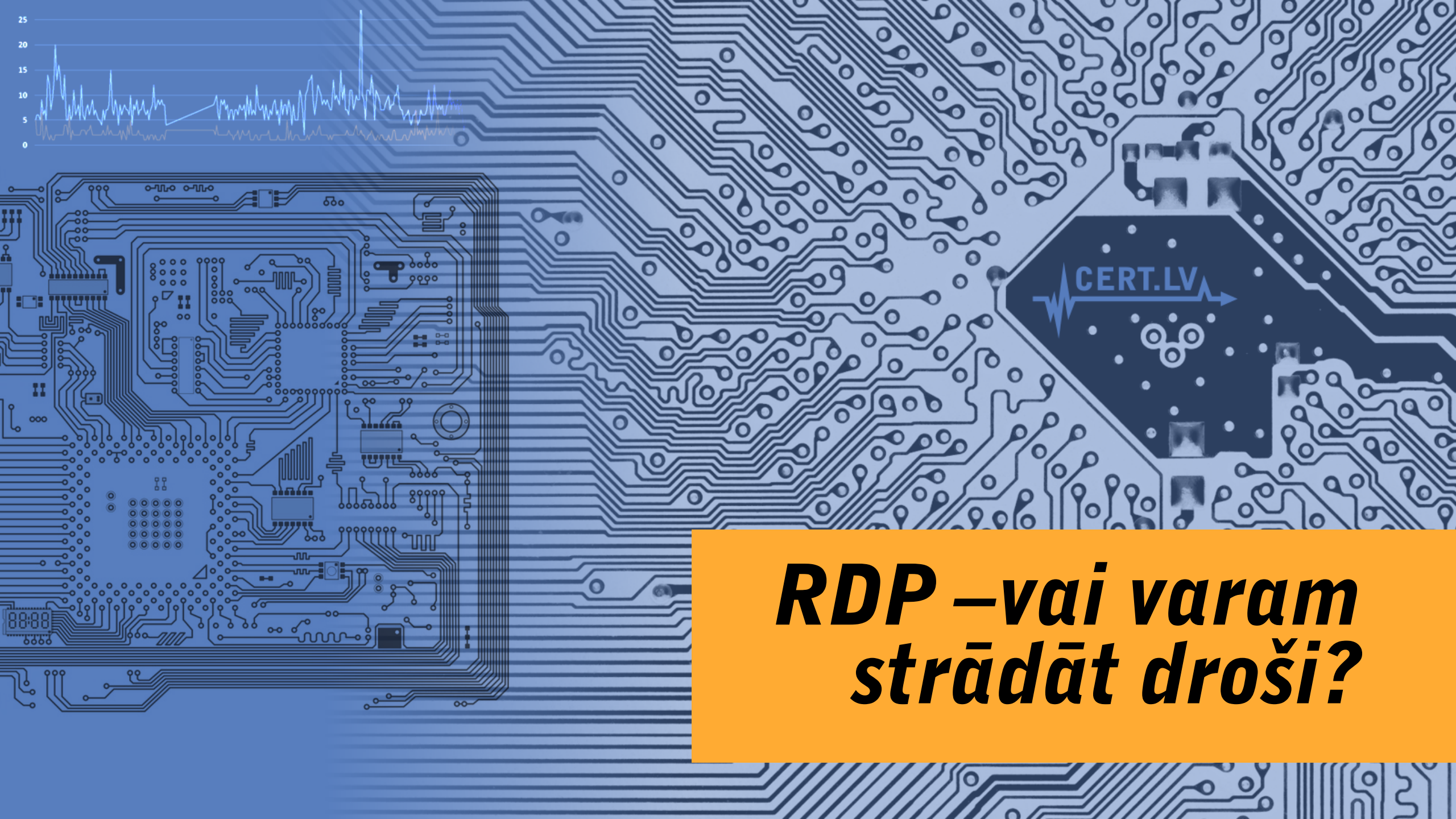
CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Attālināto pieslēgumu drošība

Gints Mālkalnietis 06.12.2018



RDP –vai varam strādāt droši?

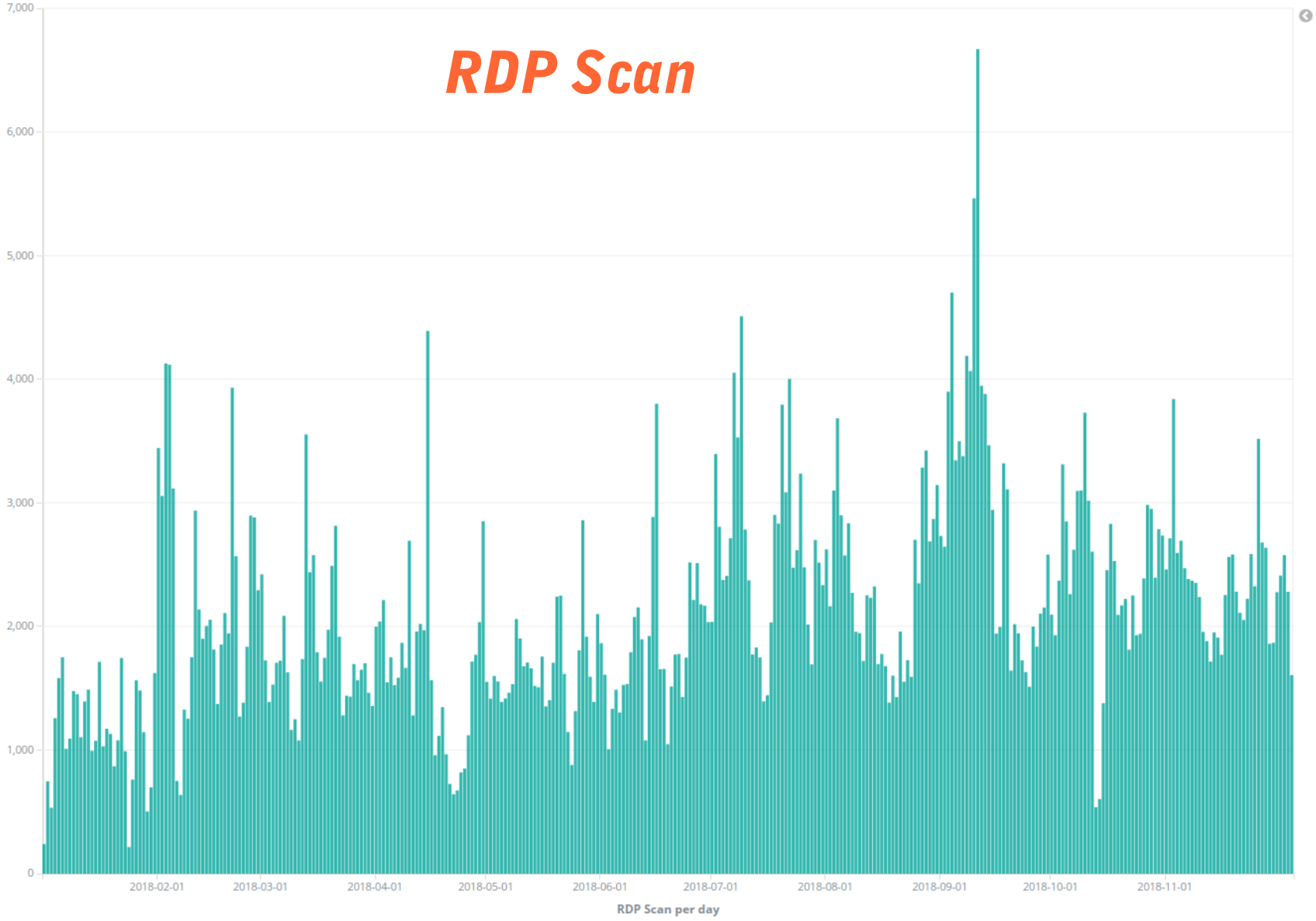
Biežāk attālināti lietotie servisi

- **RDP – Windows Remote Desktop**
- **VPN, dažādās versijās**
- **SQL server, dažādās versijās**
- **TeamViewer**
- **SSH**
- **IPMI**
- **SMB**
- **IoT, dažādi protokoli**

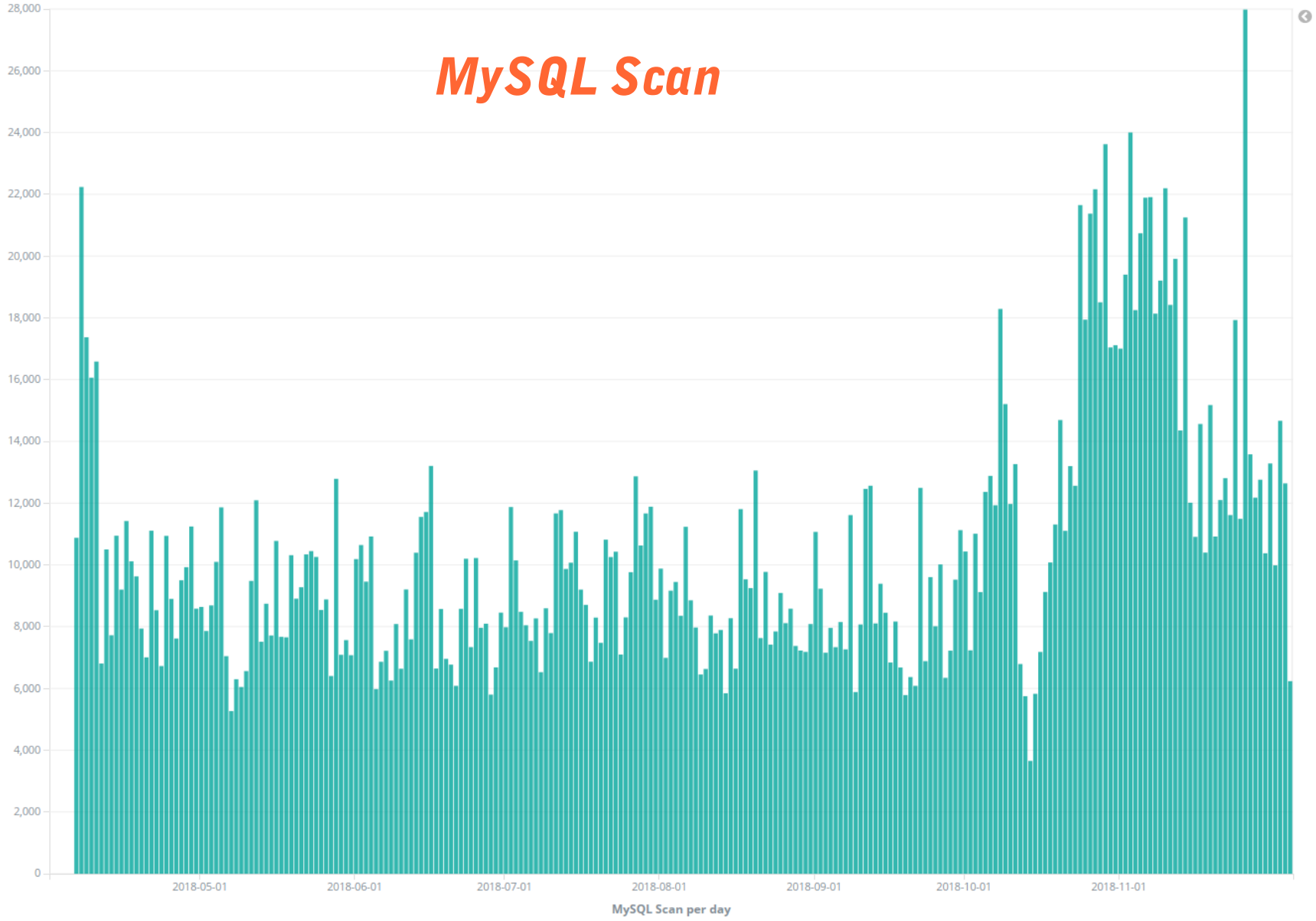
Biežāk attālināti lietotie servisi

- RDP – Windows Remote Desktop
- VPN, dažādās versijās
- SQL server, dažādās versijās
- TeamViewer
- SSH
- IPMI
- SMB
- IoT, dažādi protokoli

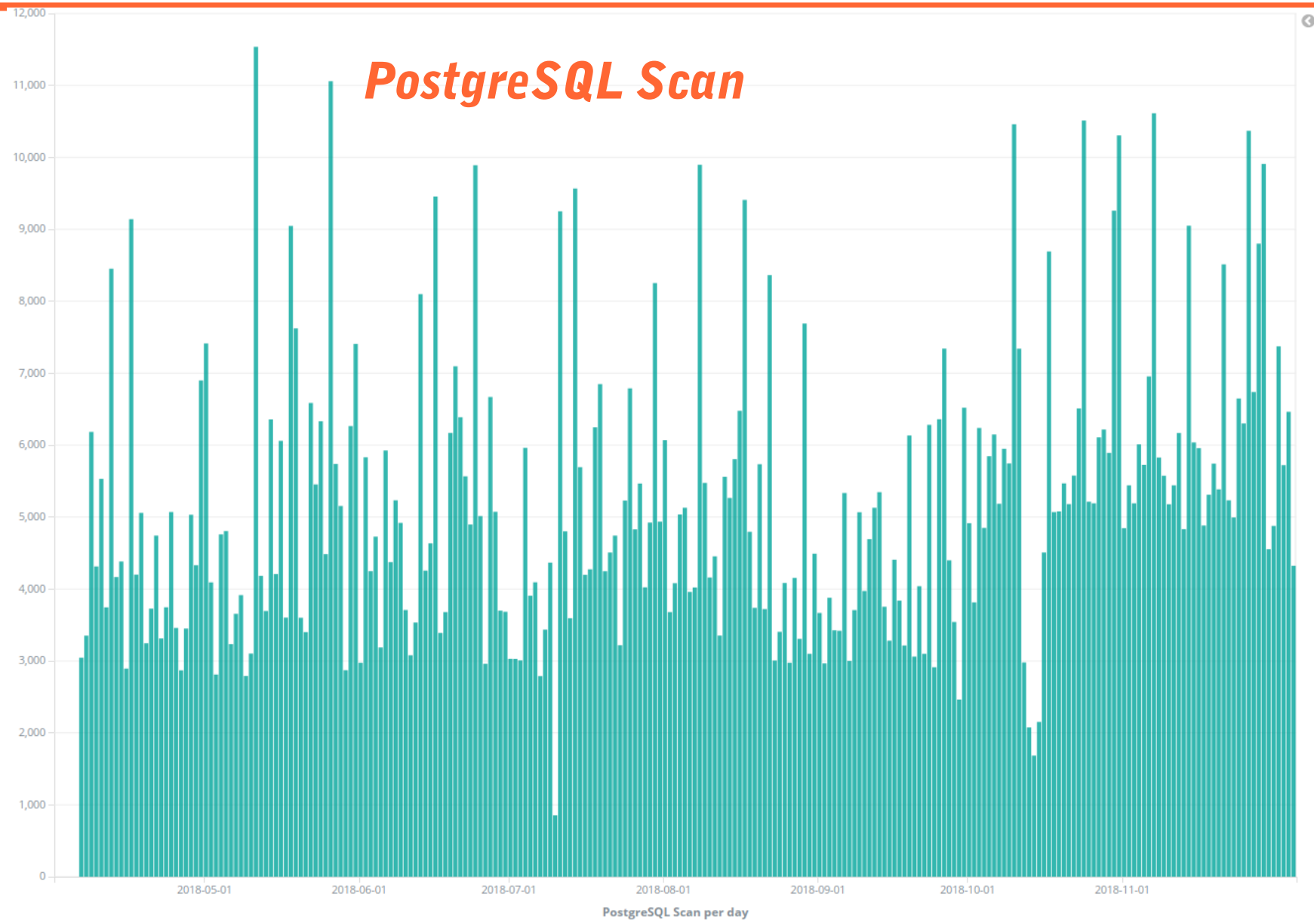
RDP Scan


7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
2018-02-01
2018-03-01
2018-04-01
2018-05-01
2018-06-01
2018-07-01
2018-08-01
2018-09-01
2018-10-01
2018-11-01
RDP Scan per day

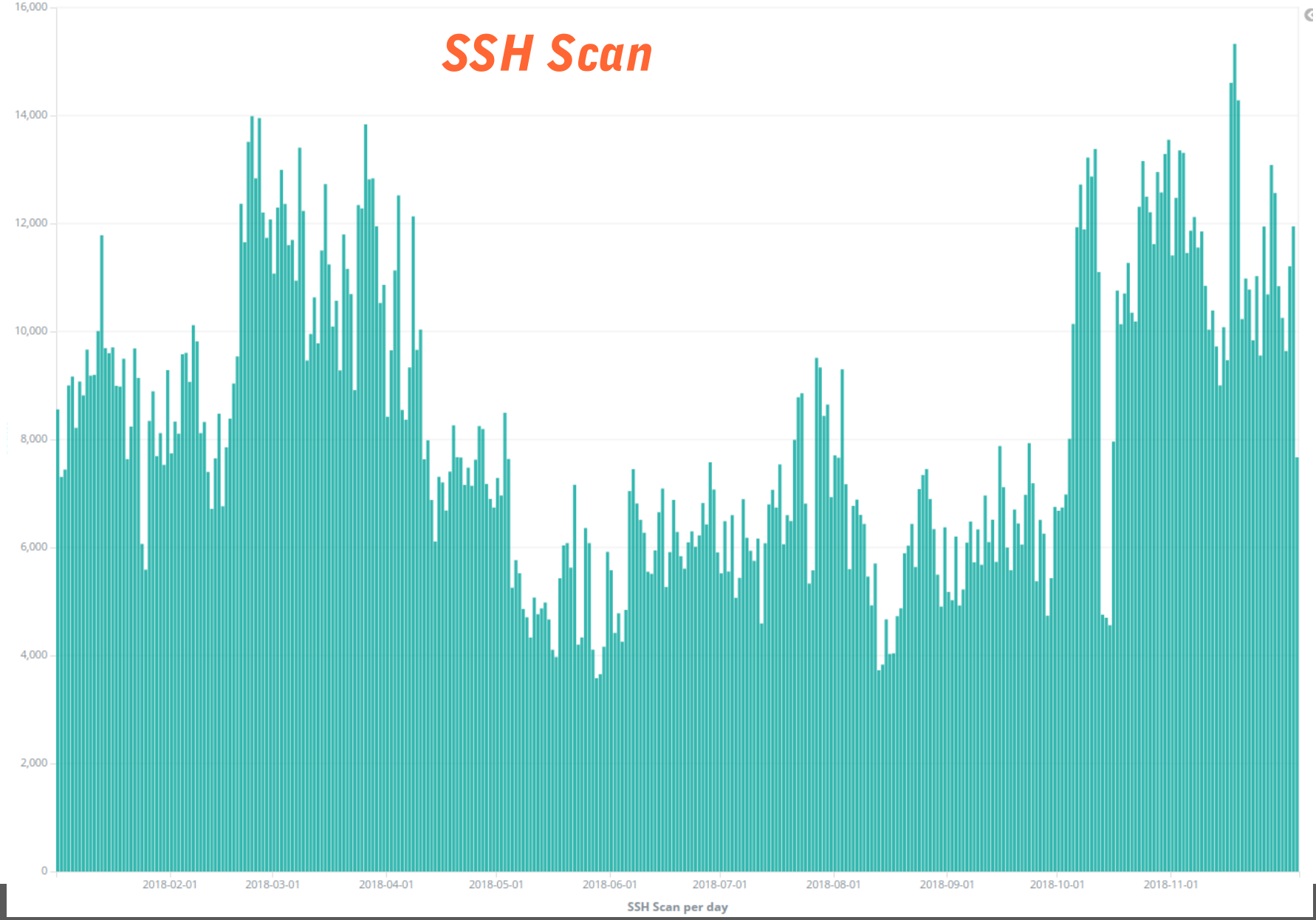
MySQL Scan

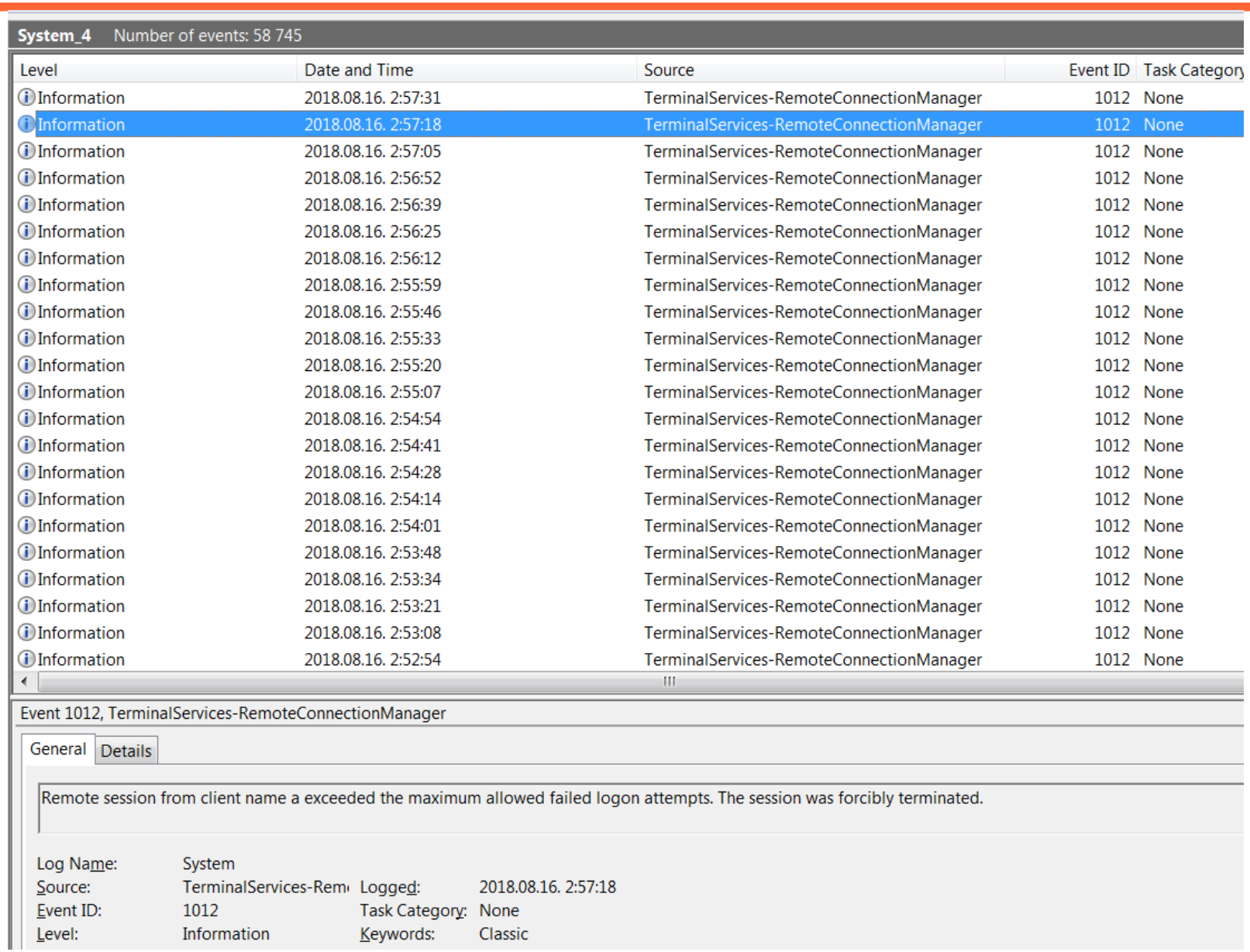

28,000
26,000
24,000
22,000
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
2018-05-01
2018-06-01
2018-07-01
2018-08-01
2018-09-01
2018-10-01
2018-11-01
MySQL Scan per day

PostgreSQL Scan



SSH Scan


16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
2018-02-01
2018-03-01
2018-04-01
2018-05-01
2018-06-01
2018-07-01
2018-08-01
2018-09-01
2018-10-01
2018-11-01
SSH Scan per day



System_4 Number of events: 58 745

Level	Date and Time	Source	Event ID	Task Category
Information	2018.08.16. 2:57:31	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:57:18	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:57:05	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:56:52	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:56:39	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:56:25	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:56:12	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:55:59	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:55:46	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:55:33	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:55:20	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:55:07	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:54:54	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:54:41	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:54:28	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:54:14	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:54:01	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:53:48	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:53:34	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:53:21	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:53:08	TerminalServices-RemoteConnectionManager	1012	None
Information	2018.08.16. 2:52:54	TerminalServices-RemoteConnectionManager	1012	None

Event 1012, TerminalServices-RemoteConnectionManager

General Details

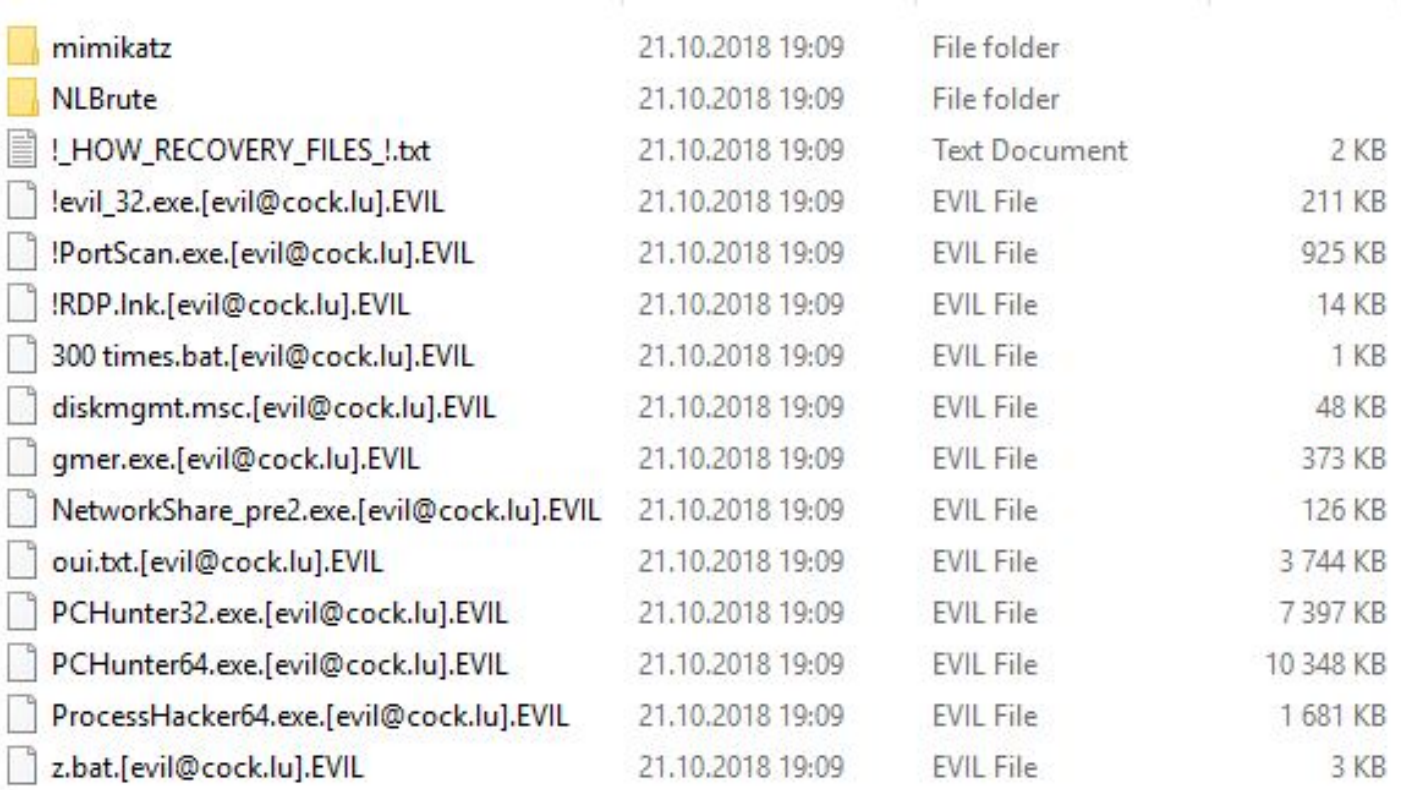
Remote session from client name a exceeded the maximum allowed failed logon attempts. The session was forcibly terminated.

Log Name:	System		
Source:	TerminalServices-Rem	Logged:	2018.08.16. 2:57:18
Event ID:	1012	Task Category:	None
Level:	Information	Keywords:	Classic

RDP – visbiežāk uzlauztais

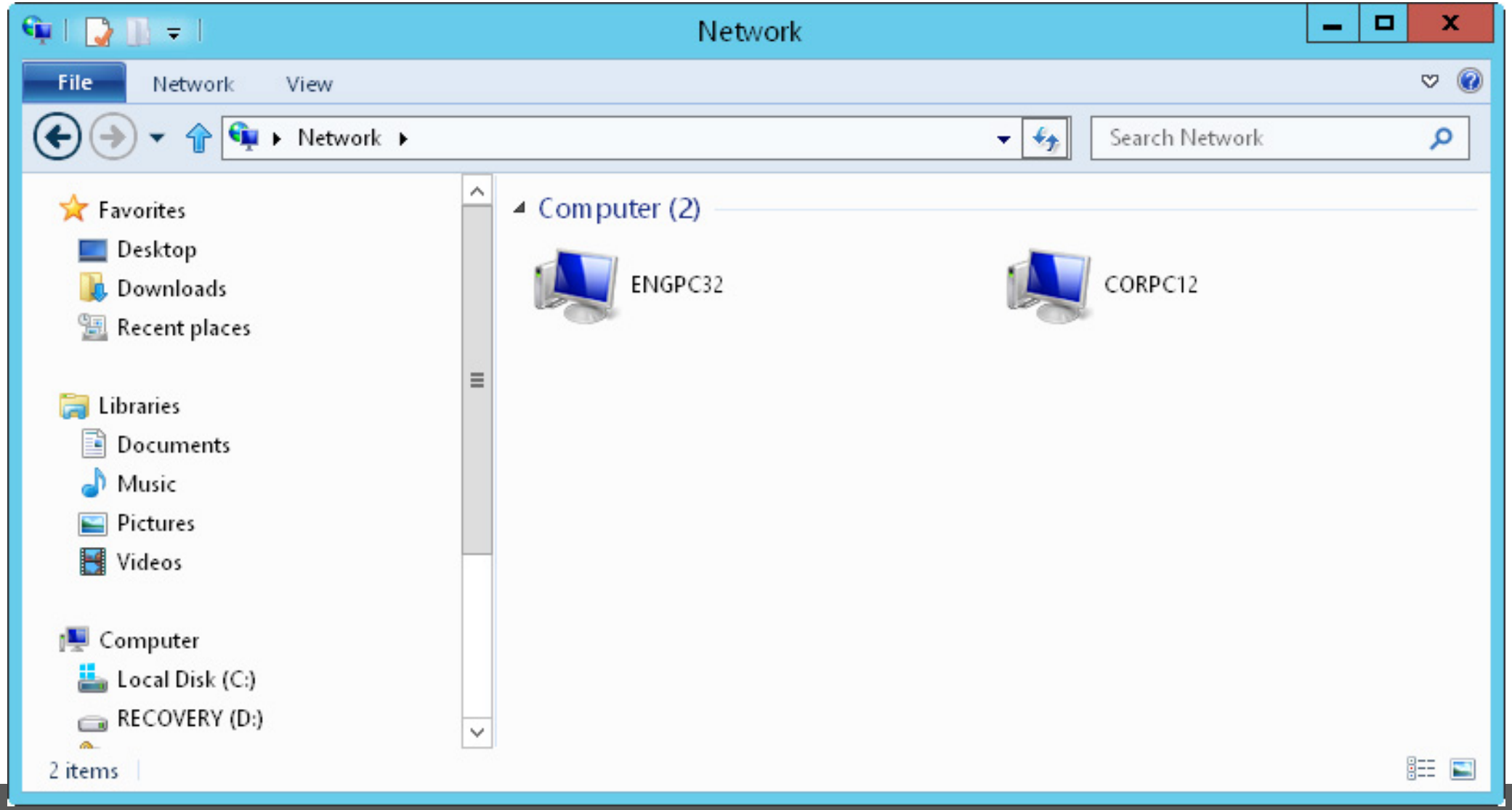
1. **Visbiežāk tiek izmantots attālināta darba veikšanai, saglabājot pilnu darbstacijas funkcionalitāti**
2. **Iecienīts grāmatvežu, projektētāju un uzņēmuma vadības lietotāju vidū**
3. **Pats RDP seviss ir kvalitatīvi programmēts, tam reģistrētas tikai 2 publiski zināmas ievainojamības, kaitīgāka no tām –** *CVE-2013-1296*
4. **Visas problēmas rodas dēļ nedrošām parolēm, un nedrošas severa konfigurācijas!**

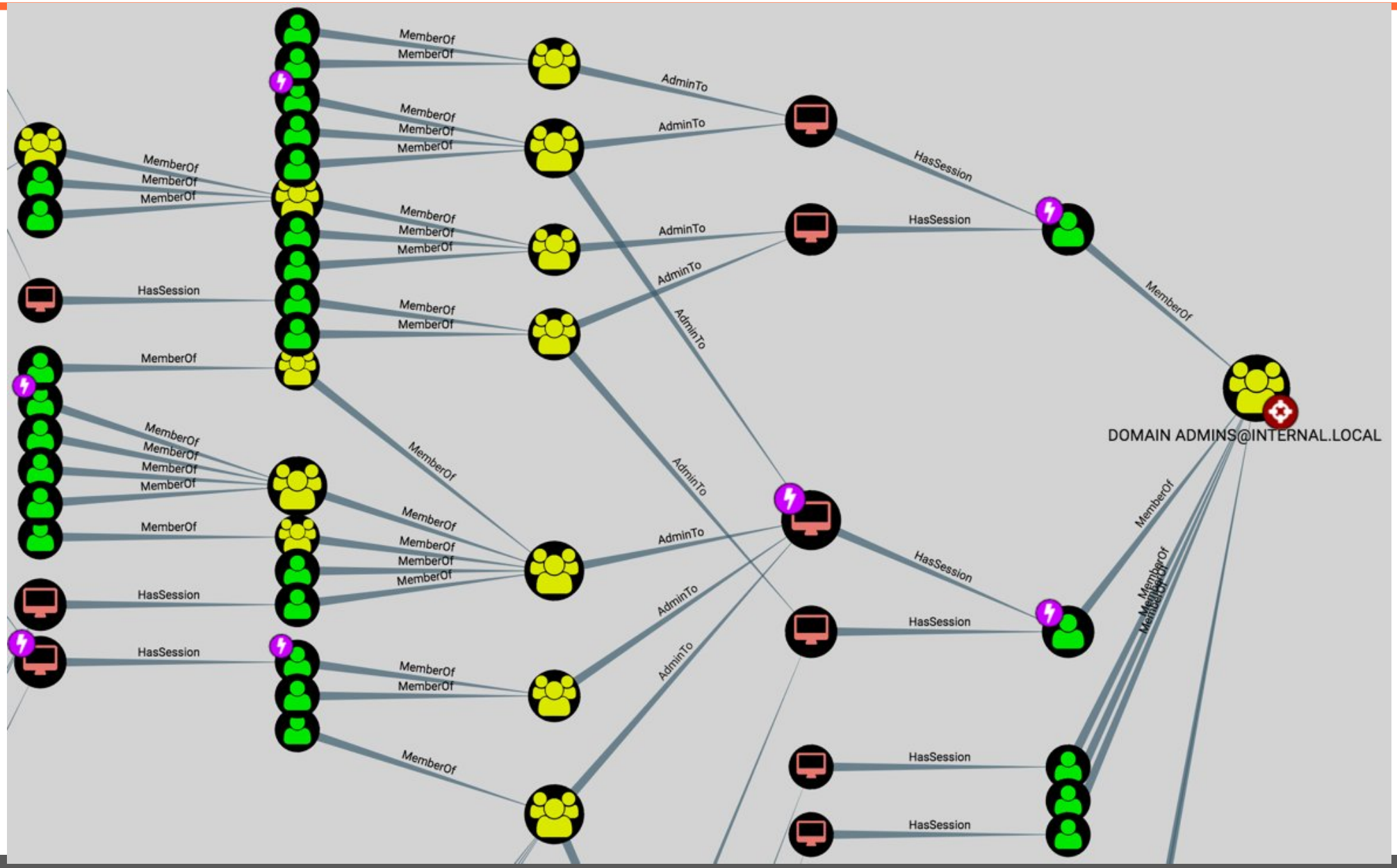
RDP – visbiežāk uzlauztais



mimikatz	21.10.2018 19:09	File folder	
NLBrute	21.10.2018 19:09	File folder	
!_HOW_RECOVERY_FILES_!.txt	21.10.2018 19:09	Text Document	2 KB
!evil_32.exe.[evil@cock.lu].EVIL	21.10.2018 19:09	EVIL File	211 KB
!PortScan.exe.[evil@cock.lu].EVIL	21.10.2018 19:09	EVIL File	925 KB
!RDP.lnk.[evil@cock.lu].EVIL	21.10.2018 19:09	EVIL File	14 KB
300 times.bat.[evil@cock.lu].EVIL	21.10.2018 19:09	EVIL File	1 KB
diskmgmt.msc.[evil@cock.lu].EVIL	21.10.2018 19:09	EVIL File	48 KB
gmer.exe.[evil@cock.lu].EVIL	21.10.2018 19:09	EVIL File	373 KB
NetworkShare_pre2.exe.[evil@cock.lu].EVIL	21.10.2018 19:09	EVIL File	126 KB
oui.txt.[evil@cock.lu].EVIL	21.10.2018 19:09	EVIL File	3 744 KB
PCHunter32.exe.[evil@cock.lu].EVIL	21.10.2018 19:09	EVIL File	7 397 KB
PCHunter64.exe.[evil@cock.lu].EVIL	21.10.2018 19:09	EVIL File	10 348 KB
ProcessHacker64.exe.[evil@cock.lu].EVIL	21.10.2018 19:09	EVIL File	1 681 KB
z.bat.[evil@cock.lu].EVIL	21.10.2018 19:09	EVIL File	3 KB

Ko tīklā redz lietotājs




MemberOf
AdminTo
HasSession
DOMAIN ADMINS@INTERNAL.LOCAL

1 solis – paroļu izveide

- **Cilvēki lieto nedrošas paroles!**
- **Ar parolēm aizsagāto kontu ir pārāk daudz, tāpēc:**
  - Izmanto īsas paroles
  - Izmanto paroles, kas ir viegli uzminamas
  - Izmanto vienu paroli vairākiem resursiem
- **Nelieto papildus autentifikācijas rīkus, pat ja tie pieejami**
  - SW kodu ģeneratori (Google autentifikators utt.)
  - Autentifikācijas aplikācijas (Smart ID utt.)
  - SMS kodi
- **Paroles garums ir kritiski svarīgs!**

2 solis -paroļu glabāšana

- **Paroles vienmēr jāglabā šifrētā veidā!**
- **Iesakām izmantot paroļu glabāšanas programmas**
  - KeePass, Last pass, 1 pass utt
  - Pieejamas dažādām OS
  - Iepējams automātiski aizpildīt paroļu laukus – turklāt, programma pārbauda ievada lauka adresi un SSL sertifikātu
  - Viegli izmantot paroles ar 20+ simboliem
- **Lielāku drošību nodrošina HW paroļu glabāšanas iekārtas**
  - Fast IDentity Online (FIDO2), Universal 2nd-factor authentication (U2F) protokoli
  - Yubikey, Google Titan utt.
  - Neaizpilda paroles nezināmās lapās
  - Tiek izstrādāti standarti, lai atteiktos no paroles vispār!

3 solis - VPN

- **Iesakām visu arējo piekļuvi uzņēmuma tīklam organizēt tikai caur VPN servisu**
- **Atkarībā no tīkla uzbūves un pieejamajām iekārtām, VPN piekļuvi var organizēt dažādos punktos:**
  - Maršrutētājs ienākošajā interneta savienojumā (Mikrotik, TPLINK utt.)
  - Speciālizēta iekārta (Cisco ASA, Zyxel Zywall)
  - Microsoft RAS
  - Dažādas citas programmas (OpenVPN utt.)
- **Lielāku drošību nodrošina iekārtas kas atbalsta vairāk, kā tikai paroli, lai nodrošinātu VPN aizsardzību**
  - X.509 sertifikāti
  - Kodu ģeneratori
  - U2F

4 solis -tīkla segmentācija

- Izplatītākie protokoli – IPsec un SSL bāzēti VPN
- SSL VPN ir mazāk izplatīti, bet darbojas no jebkura interneta savienojuma, kam ir atļauti TCP 443 SSL dati
- VPN savienojumiem ieteicams izveidot atsevišķu tīkla segmentu, ar nodalītiem resursiem un ierobežotu piekļuvi pārējām iekšējā tīkla daļām. Sadalīšanu var veikt VLAN, Windows domēna tiesību, un citos līmeņos.
- Ieteicams maksimāli ierobežot piekļuvi iekšējam tīklam, atļaujot tikai nepieciešamos servisus un aplikācijas, nevis pilnu piekļuvi.

Serviss uz nestandarta porta nav aizsardzība!

- Ieinteresēti uzbrucēji pārbaudīs visus pieejamos portus
- Regulāri jāpārbauda, kā uzņēmuma IP adrešu apgabals izskatās no interneta, vai nav jauni servisi, atvērti porti utt.
- Neuzticieties kases sistēmu, videonovērošnas iekārtu utt. pakalpojumu ieviesēju pieprasītajām tīkla konfigurācijas izmaiņām. Viņi domā tikai lai ātrāk pabeigtu savu darbu un viss strādātu. Par drošību jādomā pašiem!
- Jaunus servisus ieviešot, nesalauziet aizsardzību vecajiem!

SHODAN | remote desktop protocol -port:3389 country:"LV" | Explore | Downloads | Reports | Developer Pricing | Enterprise Access

Exploits | Maps | Images | Share Search | Download Results | Create Report

TOTAL RESULTS

55

TOP COUNTRIES

Latvia	55

TOP CITIES

Riga	29
Kuldiga	2
Talsi	1
Olaine	1
Nakotne	1

TOP ORGANIZATIONS

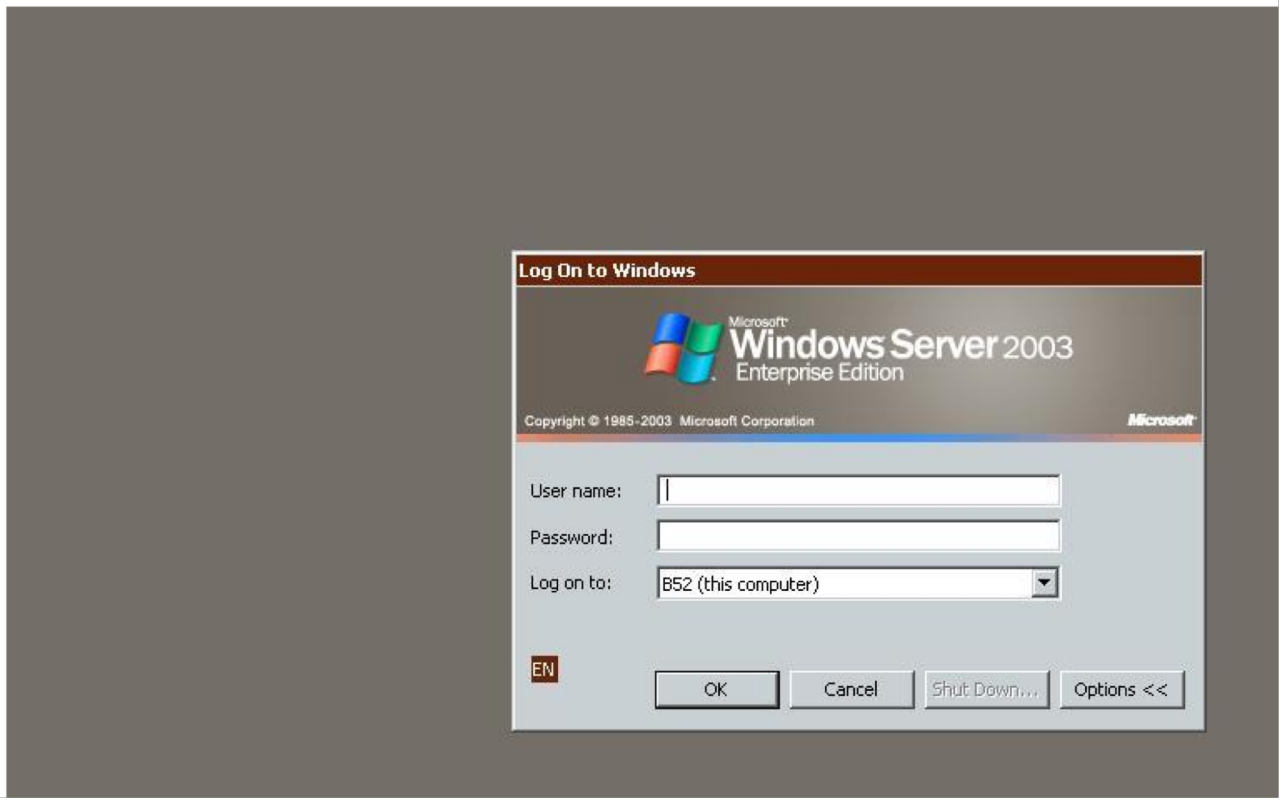
SIA Lattelecom	14
LATNET SERVISS Ltd.	7
Balticom JSC	4
Bridge Group Business Customers	3
Telia Latvija SIA	2

TOP OPERATING SYSTEMS

Windows XP	1

136.169.50.1

home-136.169.50.156.mts.lv
Windows XP
Sia Mits Lv
Added on 2018-12-04 02:50:23 GMT
Latvia, Riga
Details



Exploits | Maps | Images | Share Search | Download Results | Create Report

TOTAL RESULTS

2,201

TOP COUNTRIES

Latvia	2,201

TOP CITIES

Riga	899
Daugavpils	30
Ventspils	16
Jelgava	16
Tukums	15

TOP ORGANIZATIONS

SIA Lattelecom	447
Layer6 Networks	197
Telia Latvija Customers	79
Telia Latvija SIA	66
Makonix SIA	50

TOP OPERATING SYSTEMS

Windows XP	4
Windows 7 or 8	2

213.175.122.2

Telia Latvija Customers

Added on 2018-12-06 01:23:10 GMT

Latvia

Details

self-signed

SSL Certificate

Issued By:

|- Common Name:

lv122.kiosk.local

Issued To:

|- Common Name:

kioskpclv122.kiosk.local

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters

Fingerprint: RFC2409/Oakley Group 2

Remote Desktop Protocol

\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

185.176.221.

36.2cloud.eu

2 Cloud Ltd.

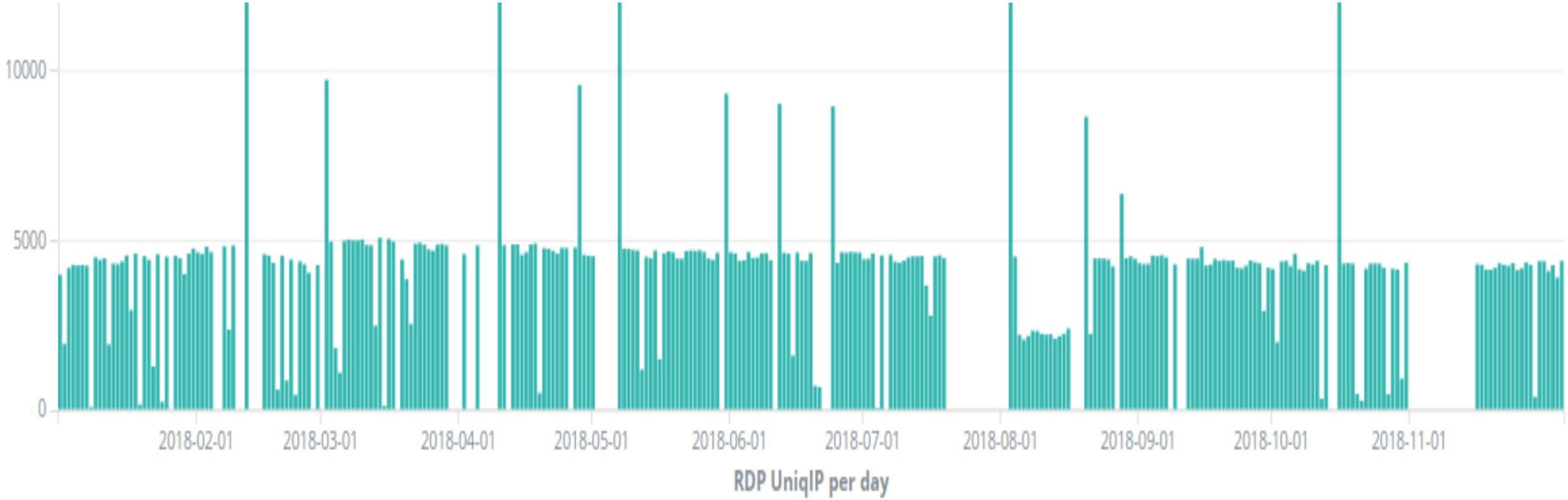
Added on 2018-12-06 01:22:03 GMT

Latvia

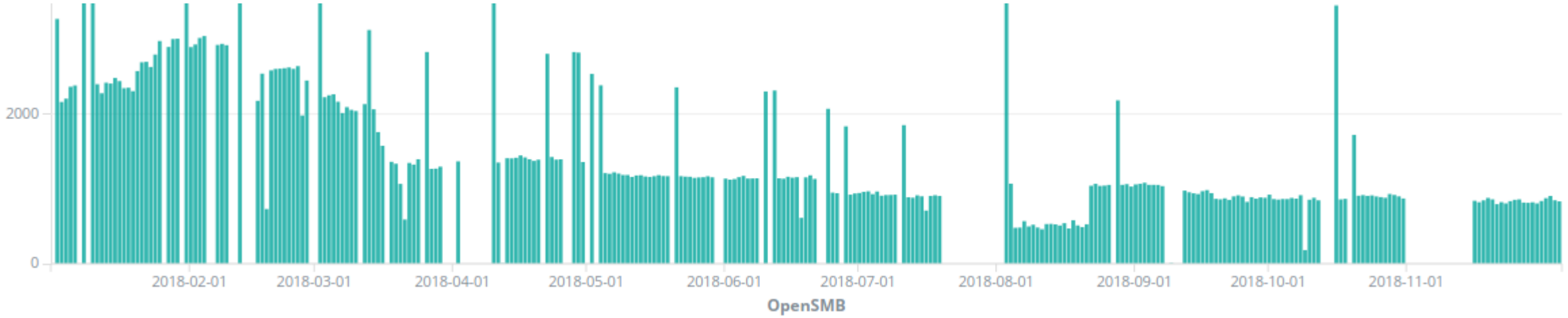
Details

self-signed

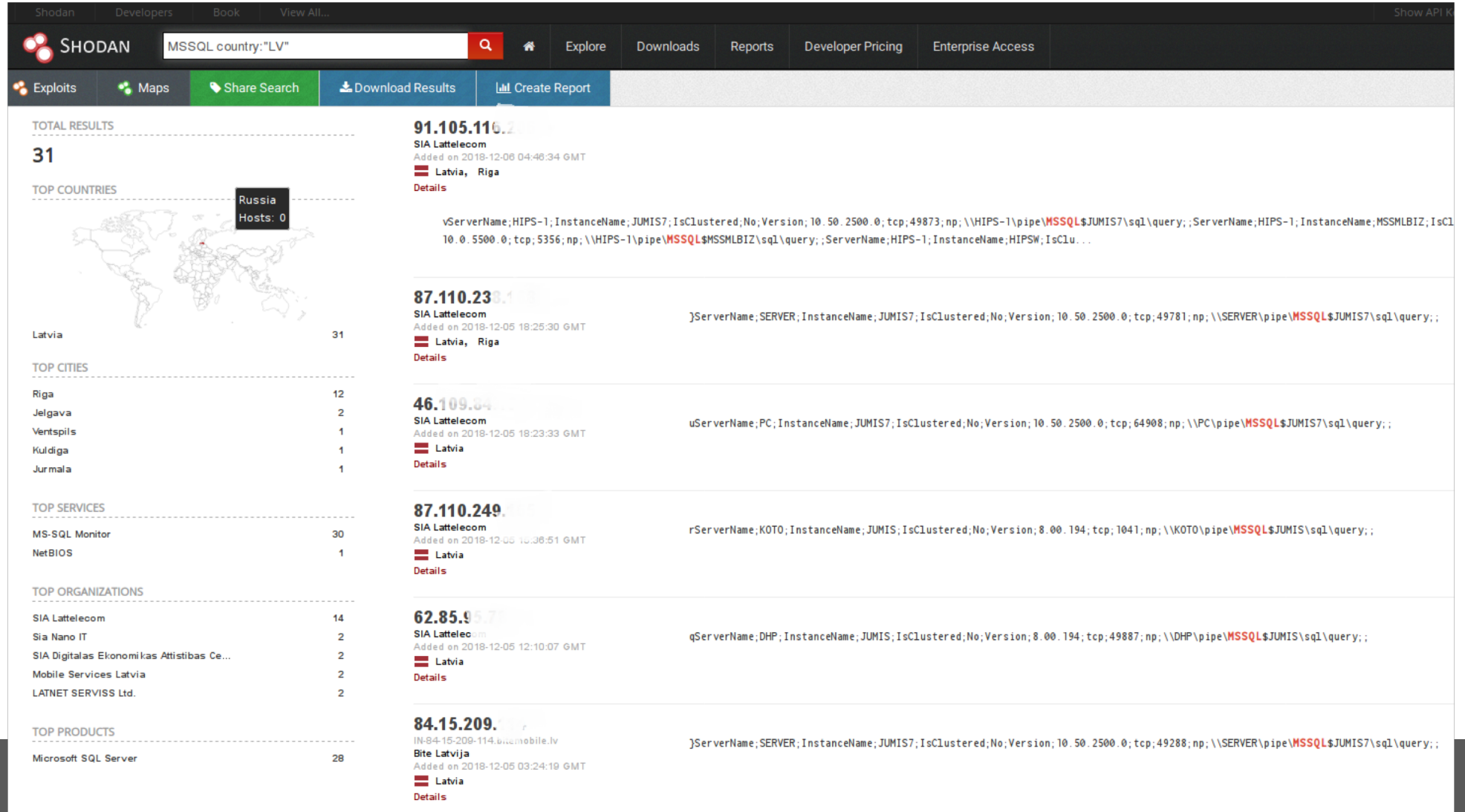
OpenRDP


10000
5000
0
2018-02-01
2018-03-01
2018-04-01
2018-05-01
2018-06-01
2018-07-01
2018-08-01
2018-09-01
2018-10-01
2018-11-01
RDP UniqIP per day

OpenSMB


2000
0
2018-02-01
2018-03-01
2018-04-01
2018-05-01
2018-06-01
2018-07-01
2018-08-01
2018-09-01
2018-10-01
2018-11-01
OpenSMB

MSSQL no grāmatvedes datora – nevajag to izlikt publiski!



MSSQL – nevajag to izlikt publiski!

- **MSSQL versija var būt novecojusi, un saturēt zināmas ievainojamības**

Microsoft SQL Server 2008 R2 (SP1) - 10.50.2500.0 (Intel X86)

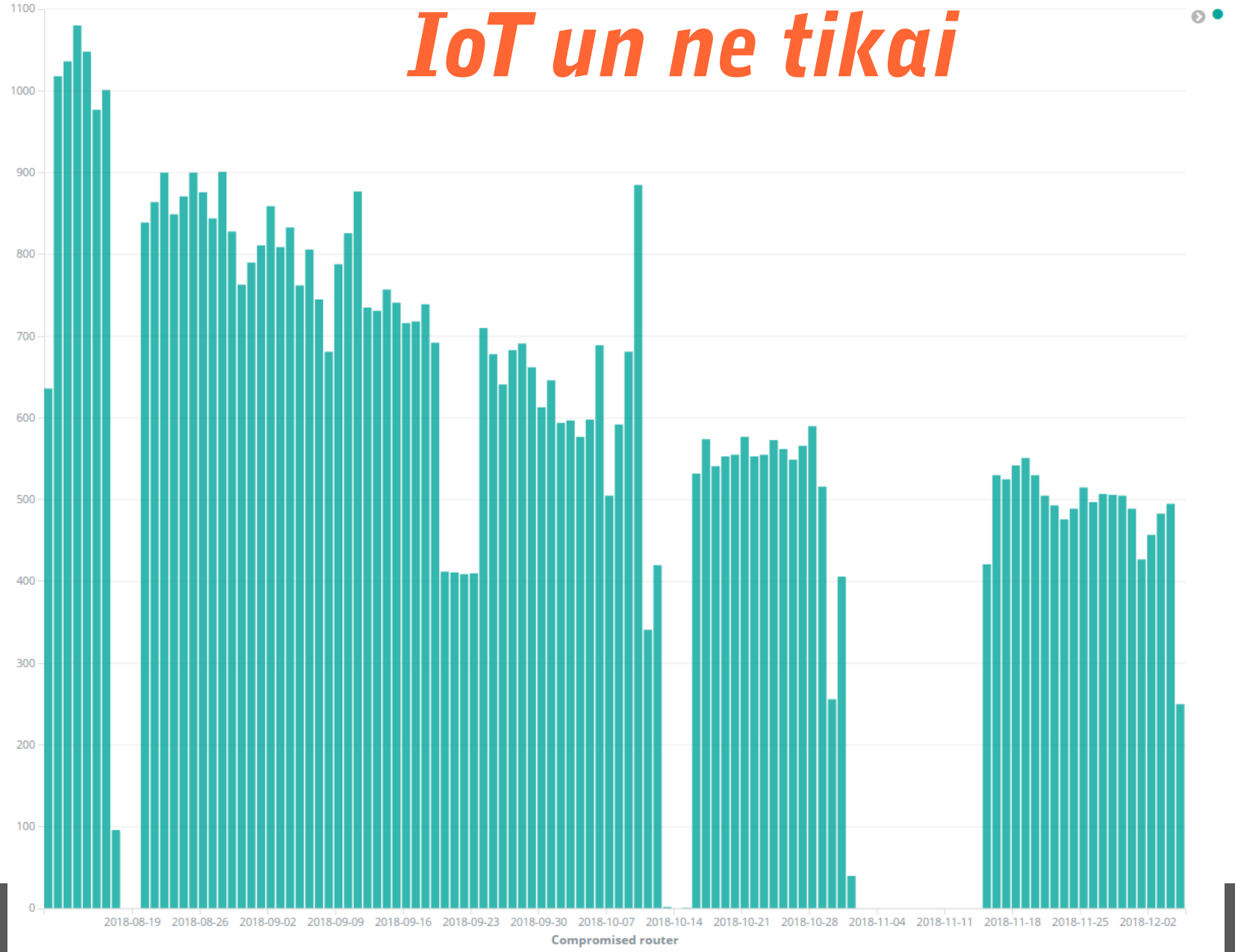
Jun 17 2011 00:57:23

Copyright (c) Microsoft Corporation

Express Edition on Windows NT 6.2 <X64> (Build 9200:) (WOW64)

- **DB SA konta parole var tikt uzminēta**
- **Ar ielēgtu Mixed Mode Authentication SA kontam var būt sistēmas administratora tiesības**

IoT un ne tikai



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

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

Thank you!

cert@cert.lv

https://www.cert.lv

certlv **certlv**