Měsíční přehled bezpečnostních incidentů

All times are displayed in the time zone UTC.

www.BezpecNej.Net

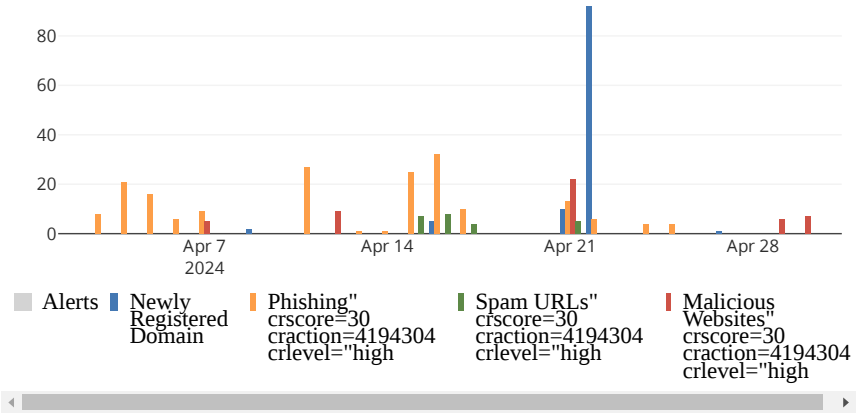
Report blokovaných kategorii bezpečnostních incidentů, URL, virů, služeb a aplikací.

Popis přehledu a incidentu naleznete zde: https://www.Sprava.IT/r/Report_bezpecnostnich_incidentu

This report uses the following parameters and values:

Parameter	Value
$VarFGT_Report_SRCIP$	(srcip:172.25.254.33)

1.1 Datum blokace a kategorie bezpečnostního incidentu



Bar chart aggregating count() by timestamp for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2024-05-01 09:23:08.

1.2 Počty blokací a kategorie bezpečnostního incidentu

catdesc	count()
Phishing" crscore=30 craction=4194304 crlevel="high	183
Newly Registered Domain	111
Malicious Websites" crscore=30 craction=4194304 crlevel="high	49
Spam URLs" crscore=30 craction=4194304 crlevel="high	24

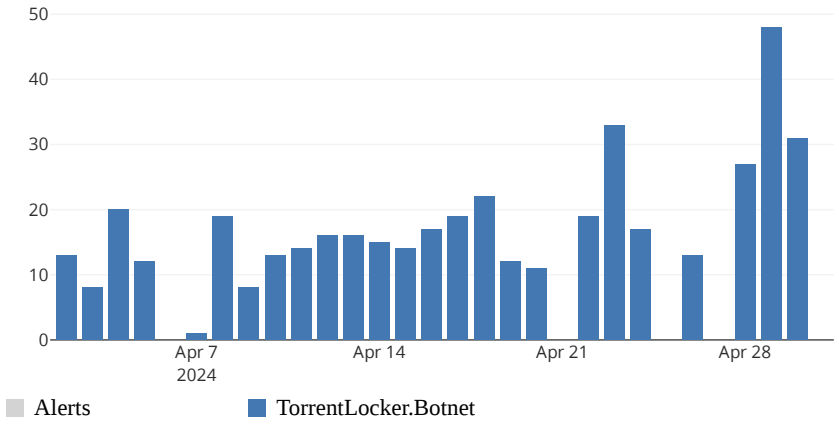
Data table aggregating count() by catdesc for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2024-05-01 09:23:07.

1.3 Typy blokací a kategorie bezpečnostního incidentu

subtype	count()
app-ctrl	67348
webfilter	367

Data table aggregating count() by subtype for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2024-05-01 09:23:07.

1.4 Datum blokace a kategorie KRITICKÉHO bezpečnostního incidentu



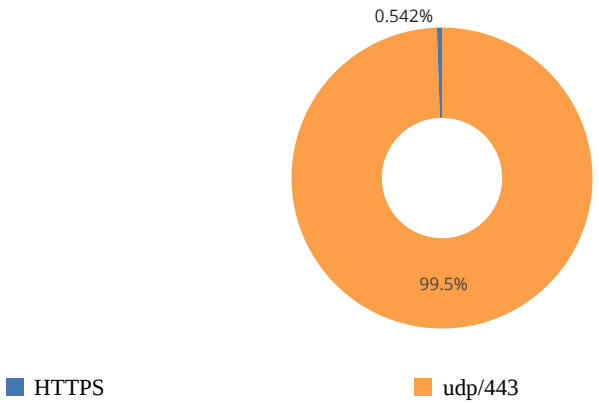
Bar chart aggregating count() by timestamp for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (subtype:ips)* and was calculated at 2024-05-01 09:23:07.

1.5 Počty blokací a kategorie KRITICKÉHO bezpečnostního incidentu

attack	count()
TorrentLocker.Botnet	438

Data table aggregating count() by attack for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$* and was calculated at 2024-05-01 09:23:08.

2.1 Blokované služby procentuálně



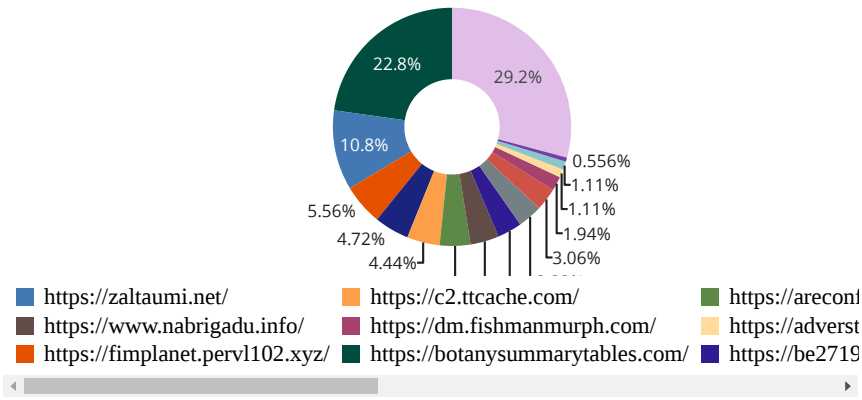
Pie chart aggregating count() by service for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2024-05-01 09:23:09.

2.2 Blokované služby / počty

service	count()
udp/443	67348
HTTPS	367

Data table aggregating count() by service for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2024-05-01 09:23:09.

3.1 Zablokované URL adresy procentuálně



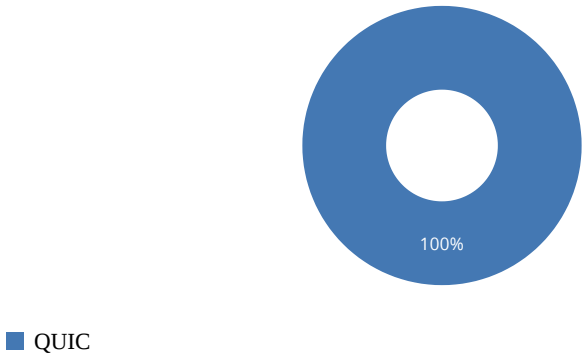
Pie chart aggregating count() by url for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2024-05-01 09:23:10.

3.2 Zablokované URL adresy / počty

url	count()
https://correlationcocktailinevitably.com/	105
https://botanysummarytables.com/	82
https://zaltaumi.net/	39
https://fimplanet.pervl102.xyz/	20
https://ci.spontonelatery.com/	17
https://c2.ttcache.com/	16
https://areconform.com/	15
https://www.nabrigadu.info/	14
https://be2719.rcr22.ams01.cdn112.com/	12
https://exposepresentimentunfriendly.com/	12
https://c4.ttcache.com/	11
https://dm.fishmanmurph.com/	7
https://adverster.g2afse.com/	4
https://track.tracknsetr.com/	4
https://cz-prelands.com/	2

Data table aggregating count() by url for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block) AND NOT dstcountry:Reserved* and was calculated at 2024-05-01 09:23:10.

4.1 Blokované aplikace procentuálně



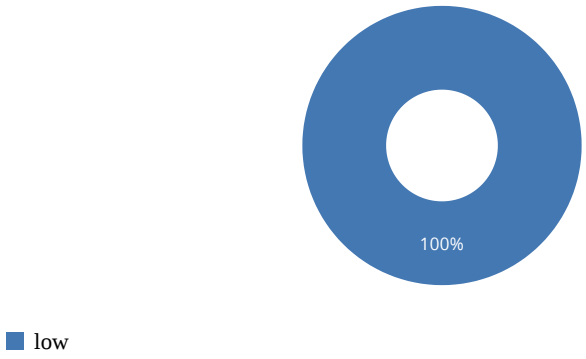
Pie chart aggregating count() by app for messages in stream *Fortigate Application Control Logs = type:utm subtype:app-ctrl* from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2024-05-01 09:23:10.

4.2 Blokované aplikace / počty

app	count()
QUIC	67348

Data table aggregating count() by app for messages in stream *Fortigate Application Control Logs = type:utm subtype:app-ctrl* from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2024-05-01 09:23:11.

4.3 Blokované aplikace podle rizikovosti procentuálně



Pie chart aggregating count() by apprisk for messages in stream *Fortigate Application Control Logs = type:utm subtype:app-ctrl* from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2024-05-01 09:23:11.

4.4 Blokované aplikace podle rizikovosti počty

apprisk	count()
low	67348

Data table aggregating count() by apprisk for messages in stream *Fortigate Application Control Logs = type:utm subtype:app-ctrl* from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2024-05-01 09:23:12.

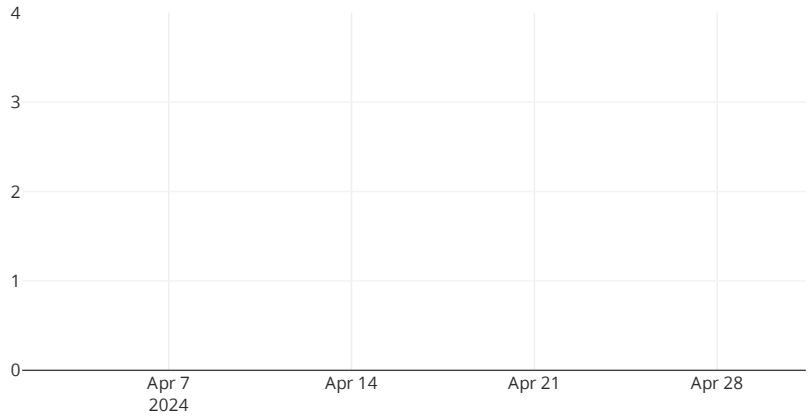
4.5 Počet blokovaných incidentů

67343

+12,963 / +23.84%

Single number aggregating count(critical) for messages in stream *Fortigate Application Control Logs = type:utm subtype:app-ctrl* from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND (action:deny OR action:blocked OR action:block)* and was calculated at 2024-05-01 09:23:12.

5.1 Blokované viry v čase



Bar chart aggregating count() by timestamp for all messages from 30 days ago until now. The visualization represents data for query *$VarFGT_Report_SRCIP$ AND subtype:virus AND action:blocked* and was calculated at 2024-05-01 09:23:13.