CYBER INCIDENTS RESPONSE OPERATIONAL CENTRE
OF THE STATE CYBER PROTECTION CENTRE
OF THE STATE SERVICE OF SPECIAL COMMUNICATION
AND INFORMATION PROTECTION OF UKRAINE

2022

REPORT

ON VULNERABILITY DETECTION AND CYBER INCIDENTS/ CYBER ATTACKS RESPONSE SYSTEM

TLP:WHITE

VULNERABILITY DETECTION AND CYBER INCIDENTS/CYBER ATTACKS RESPONSE SYSTEM

is a set of software and software-hardware tools that ensure round-the-clock monitoring, analysis and transferring of telemetric information about cyber incidents and cyber attacks which occurred or are currently occurring at cyber protection objects and may have negative impact on their sustainable functioning.

SUBSYSTEM OF CYBER INCIDENTS RESPONSE OPERATIONAL CENTRE

is a central component of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System and provides:

- centralized management of all subsystems of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System;
- centralized collection and accumulation of information about network information security events;
- real-time monitoring and processing of cyber threats and cyber incidents.

The Subsystem of Cyber Incidents Response Operational Centre detects malicious activity, as well as system and network anomalies at cyber protection objects by analysing the data, which is received from network devices (active sensors, firewalls, vulnerability scanners), workstations and servers, authorization systems, internal and external cyber threats data sources.

MONITORING STATISTICS

QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA

registered cyber incidents

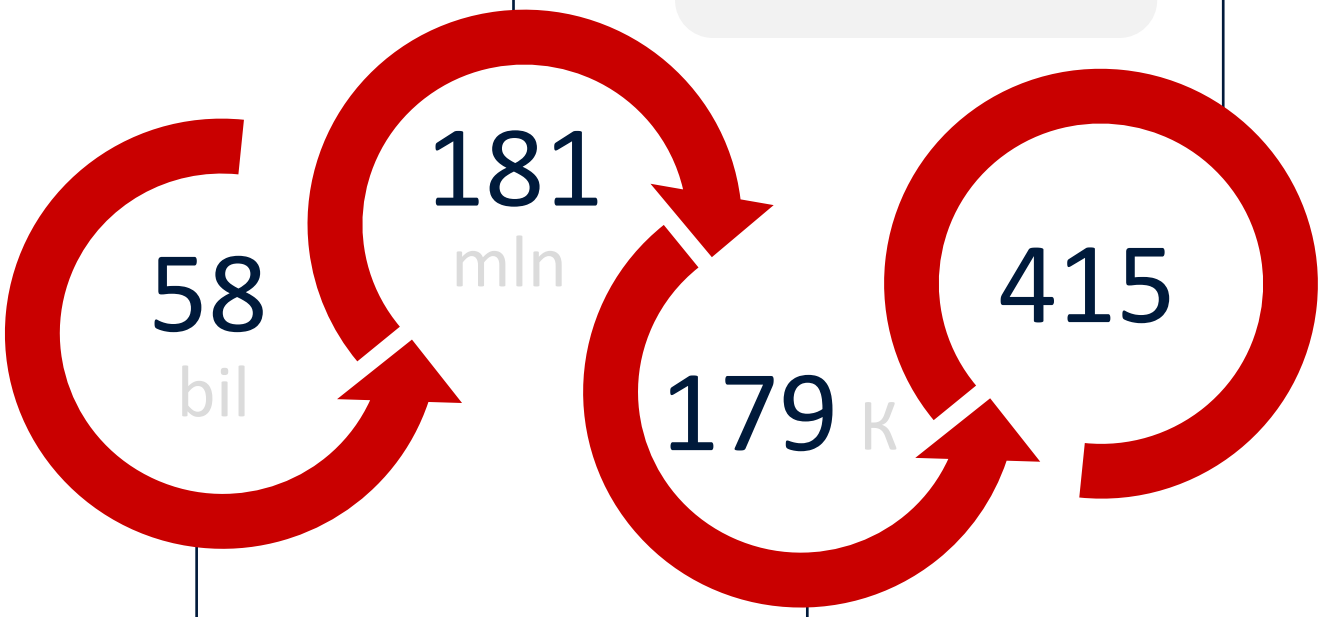
critical IS events identified and processed directly by security analysts

↑2.8

times more cyber incidents were registered (comparing to the same time period during 2021).

detected suspicious IS events

during primary analysis



processed events

received by means of monitoring, analysis and transferring of telemetric information about cyber incidents and cyber attacks

processed critical IS events

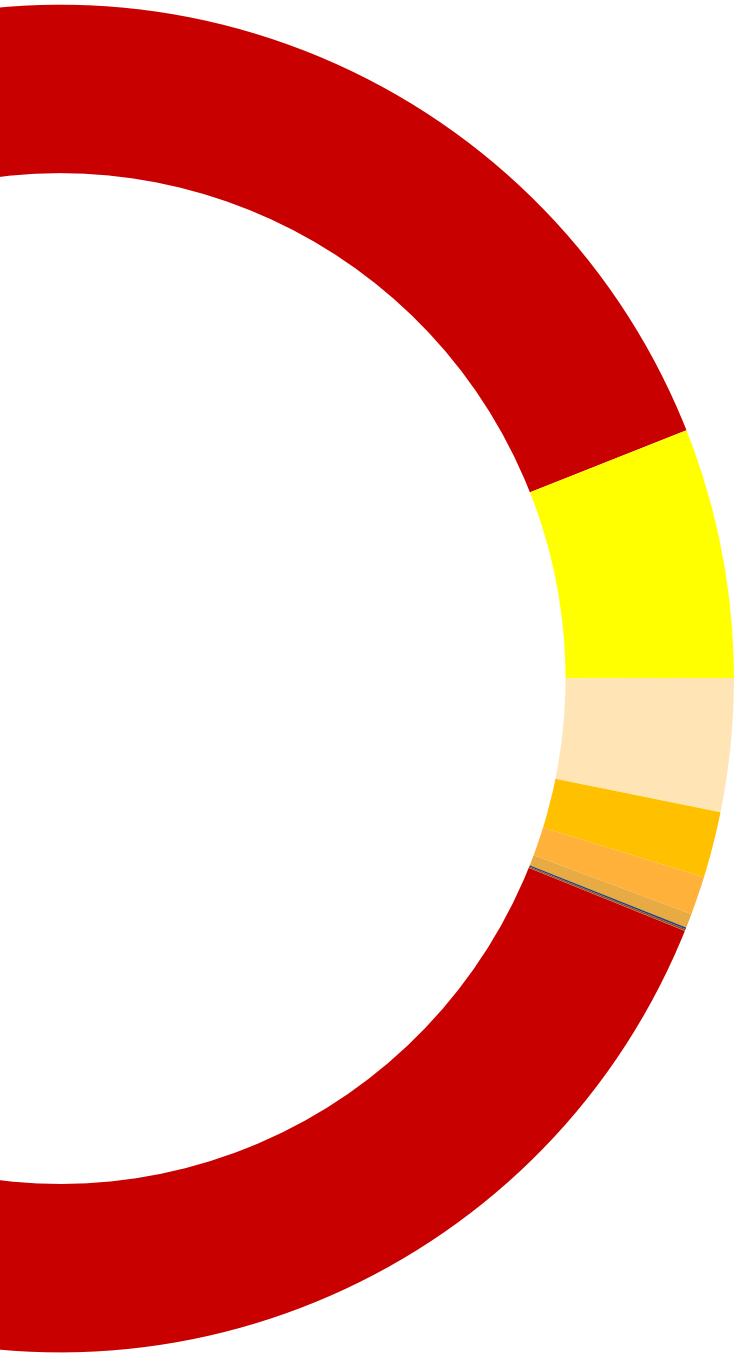
potential cyber incidents identified after suspicious IS events filtering and secondary analysis completion

IS EVENTS MONITORING

QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA

displayed according to Incident Classification Taxonomy

approved by the National Coordination Center for Cybersecurity under the National Security and Defense Council of Ukraine



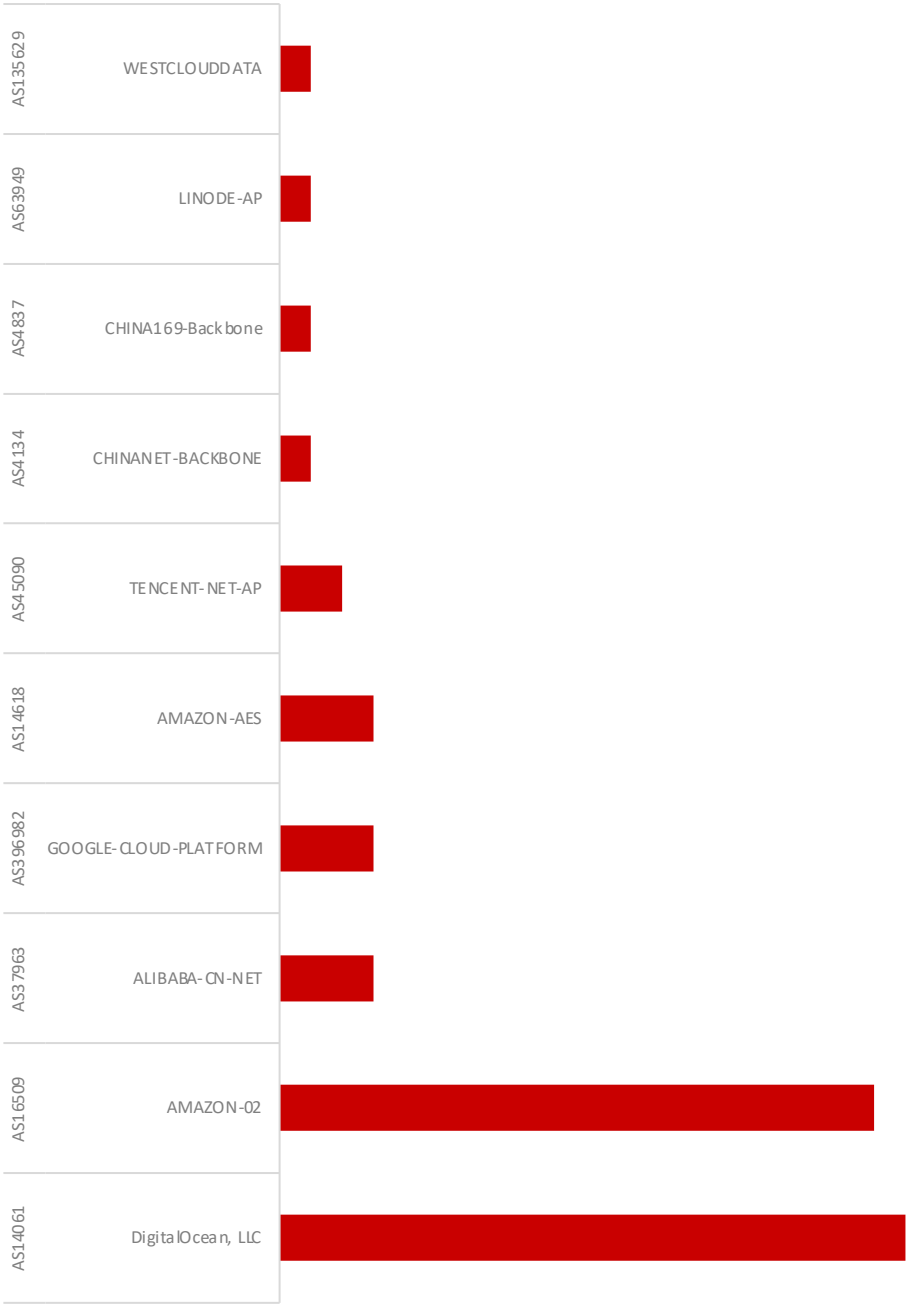
- 02 Malicious Code
- 03 Information Gathering
- 04 Intrusion Attempts
- 10 Other
- 08 Fraud
- 07 Information Content Security
- 06 Availability
- 09 Vulnerable
- 05 Intrusion
- 01 Abusive Content

↑18.3 ,↑2.2

by such amount of % accordingly the number of IS events in categories «02 Malicious Code», «03 Information Gathering» increased (comparing to the same time period during 2021)

Top 10 source ASN

the chart displays top 10 ASN (in percent ratio), the dominant number of IP addresses of which were identified as active scanning sources for the reporting period



Top 10 source IPs

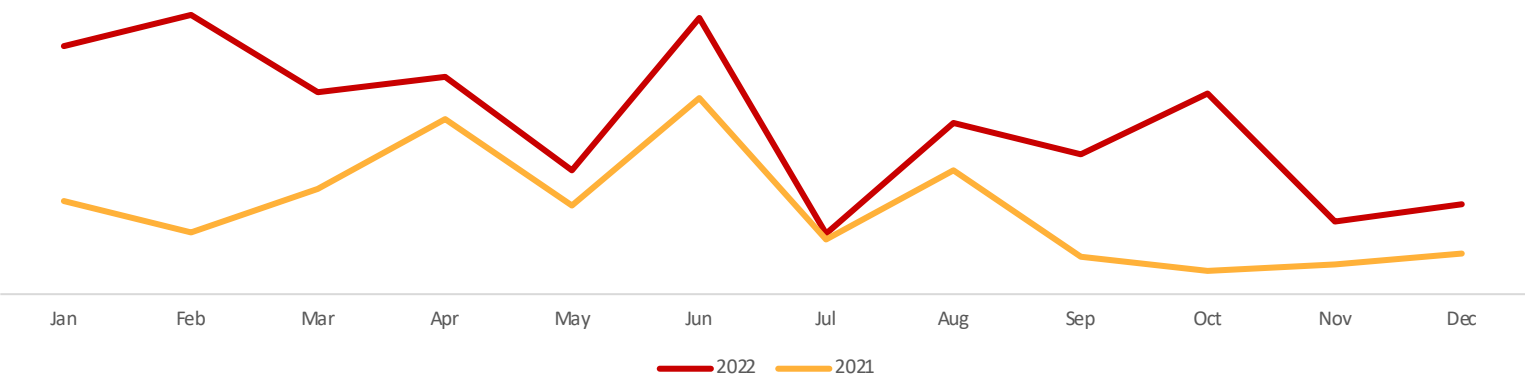
the chart displays top 10 IP addresses (in percent ratio), which were identified as active scanning sources for the reporting period

src	src country	AS NUMBER	AS NAME	%
45.93.16.71	Germany	AS23470	ReliableSite	0,40
206.189.5.99	Netherlands	AS14061	DIGITALOCEAN-ASN	0,38
89.248.165.199	Netherlands	AS202425	IP Volume inc	0,32
72.167.32.184	United States	AS398101	GoDaddy	0,31
185.156.73.91	russian federation	AS44446	OOO SibirInvest	0,30
97.74.81.123	Singapore	AS26496	GoDaddy	0,29
60.161.81.116	China	AS4134	Chinanet	0,26
93.174.93.227	Netherlands	AS202425	IP Volume inc	0,23
146.88.240.4	United States	AS20052	NETSCOUT Arbor	0,22
45.143.200.114	russian federation	AS212283	Roza Holidays Eood	0,21

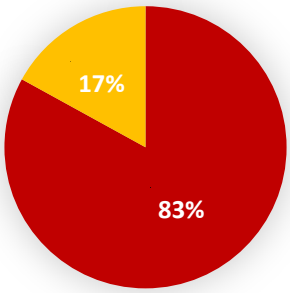
87 389

unique suspicious files were automatically detected during the reporting period
by the Subsystems of the
Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System

Timechart of malware distribution activity



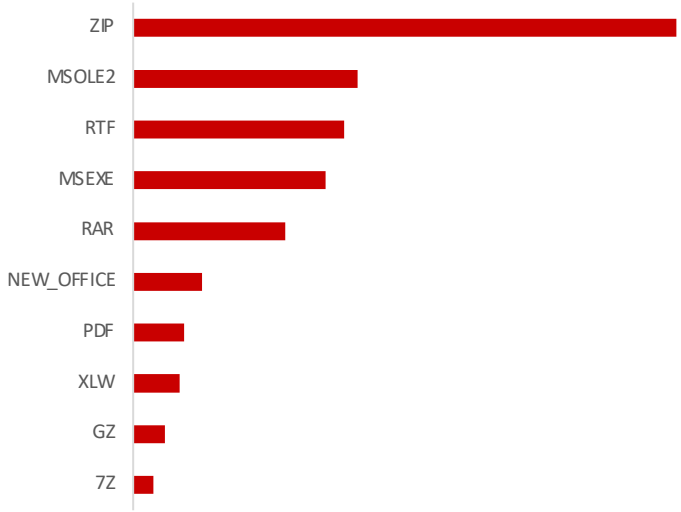
Malware distribution activity by source



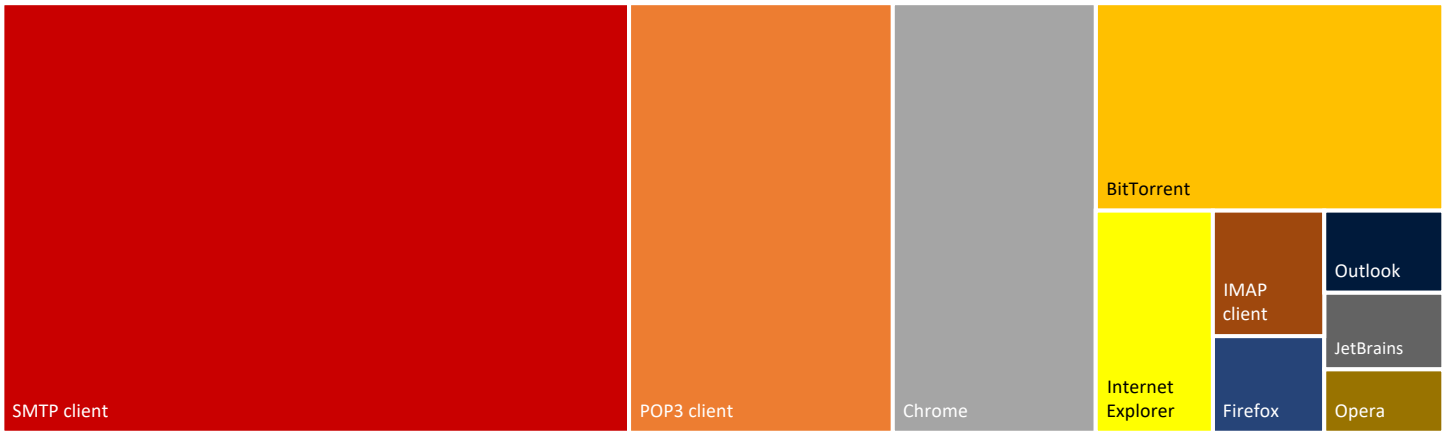
network — alerts from the Endpoint Detection and Response Subsystem on the level of user and server workstations about detecting malicious activity on them

endpoint — network events from the Telemetry Collection Subsystem, that identify malware distribution by HTTP, SMTP, POP3, IMAP protocols

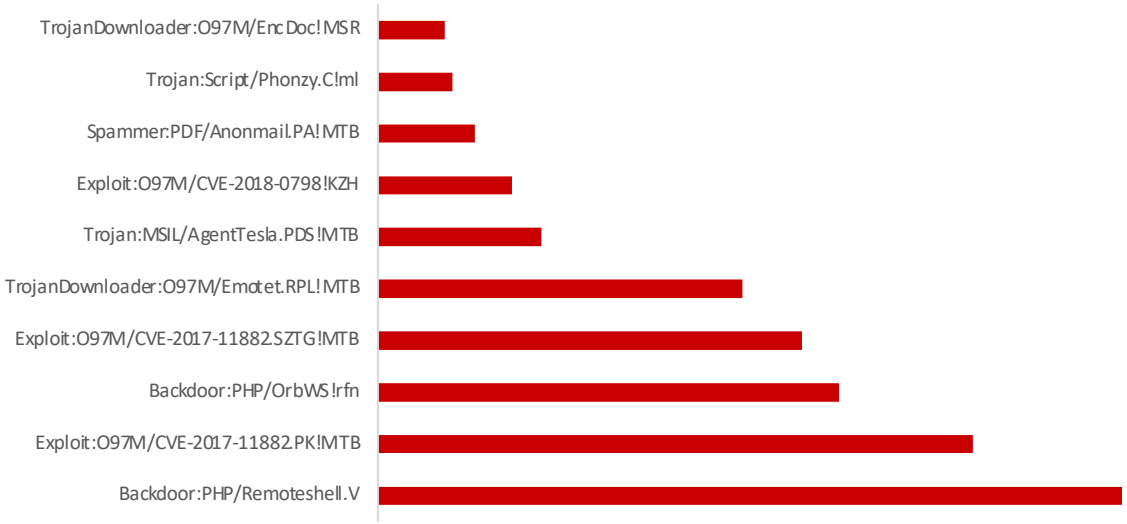
By malware files extentions



By associated software, used as a malware distribution channel



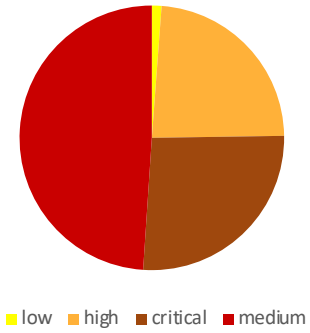
By malware files signatures



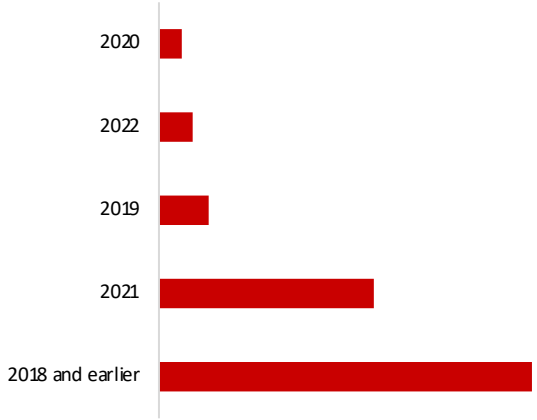
presented charts display statistical information for the reporting period, obtained by analysing IS events, which were triggered by intrusion attempts of all priorities targeted on the networks of cyber protection objects and the realization of cyber threats with the aim of detecting software vulnerabilities, finding misconfigurations of services and active network devices

Qualitative rating by CVSS Base Score

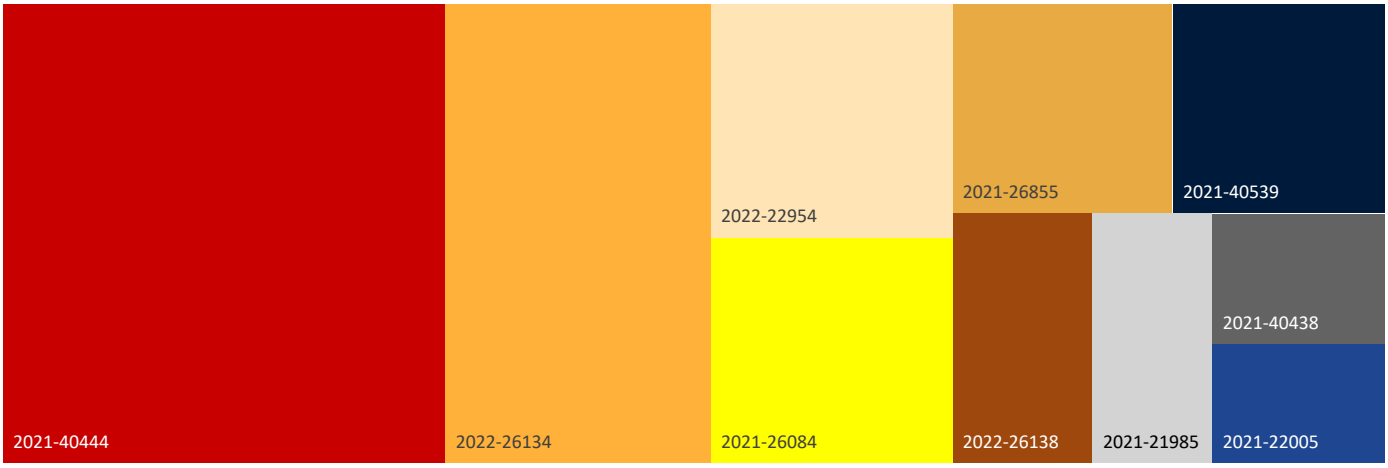
according to the approach of comparing CVSS Base Scores (1-10) to a qualitative rating scale, described in CVSSv3.1 specification



Top exploited vulnerabilities by year



Top 10 exploited vulnerabilities

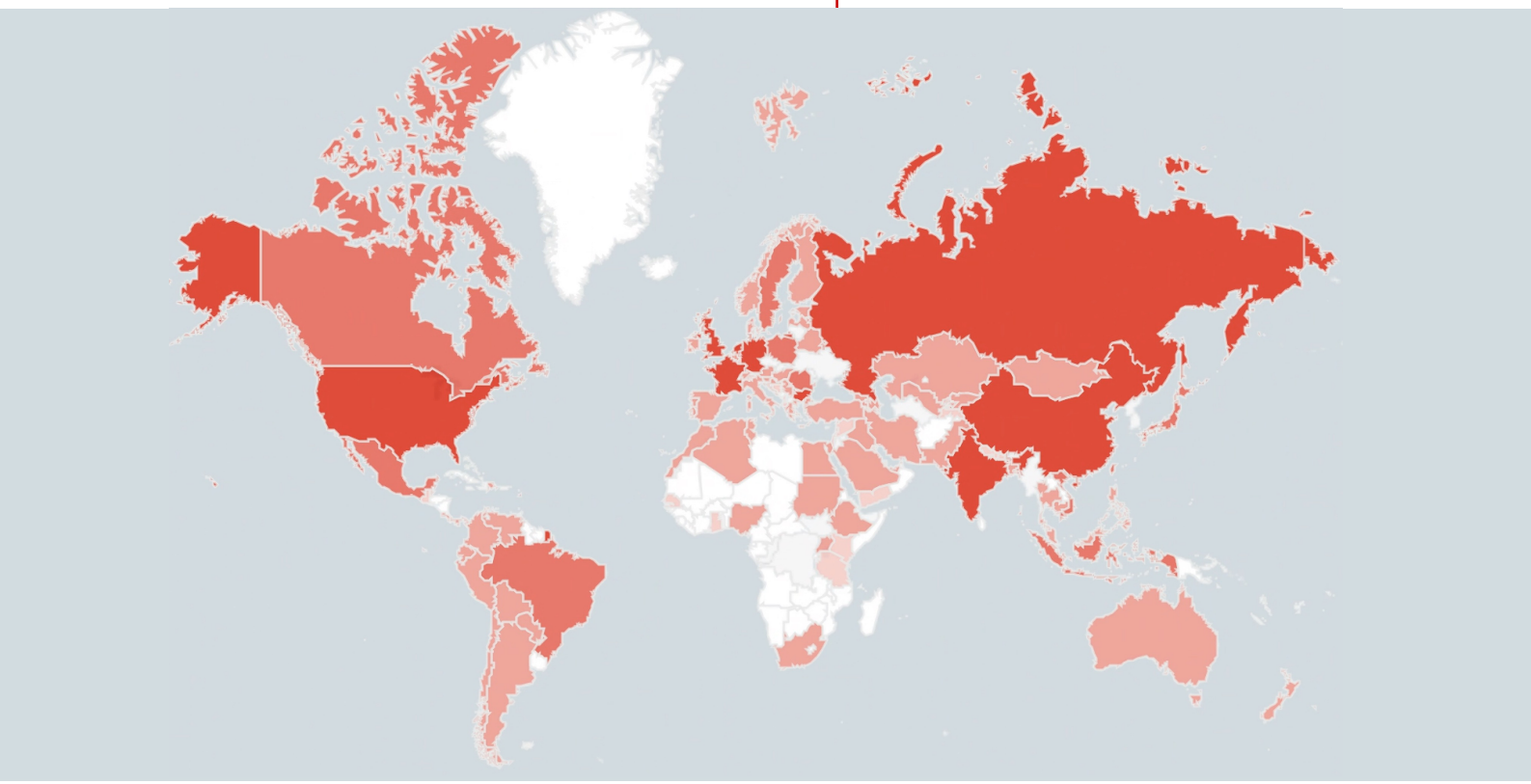


GEOGRAPHY OF DETECTIONS

OF CRITICAL INFORMATION SECURITY EVENTS *

↑26%

by such amount of % the number of critical IS events were detected, that originate from russian IP addresses
(comparing to the same time period during 2021)



*automatically determined geolocation of source IP addresses of critical IS events does not necessarily mean their attribution to the identified location

CONTACTS

Cyber Incidents Response Operational Centre

State Cyber Protection Centre

State Service of Special Communication and Information Protection of Ukraine

e-mail: soc@scpc.gov.ua
tel.: +38 (044) 281 87 37