2022(Q1)

SECURITY OPERATION CENTRE
OF THE STATE CYBER PROTECTION CENTRE
OF THE STATE SERVICE OF SPECIAL COMMUNICATION
AND INFORMATION PROTECTION OF UKRAINE

REPORT ON THE PERFORMANCE OF THE VULNERABILITY DETECTION AND CYBER INCIDENT RESPONSE SYSTEM

TLP:WHITE

STATISTICS

SECURITY OPERATION CENTRE
OF THE STATE CYBER PROTECTION CENTRE
UNDER THE STATE SERVICE OF SPECIAL
COMMUNICATION AND INFORMATION PROTECTION

SUBSYSTEM OF THE SECURITY OPERATION CENTRE

is an element of the vulnerability detection and cyber incident response system that enables the following:

- centralized collection and accumulation of network event data related to information security
- centralized management of all subsystems within the vulnerability detection and cyber incident response system
- real-time monitoring and processing of cyber threats and cyber incidents

The SECURITY OPERATION CENTRE's subsystem detects harmful activity as well as system and network anomalies at cyber defense facilities by analyzing the data obtained from network devices (active sensors, firewalls, vulnerability scanners), workstations and servers, authorization systems, internal and external cyber threat data sources.

AMOUNT OF COLLECTED AND PROCESSED DATA

hosts **≈ 15.3 k**

FPS **≈ 20 k**

traffic **≈ 50 Gbit/s**

SIEM incoming traffic

≈ 70 Gb/d

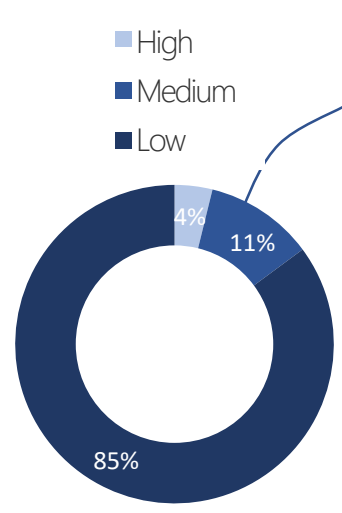
incoming data (flow) received

≈ 13 bln

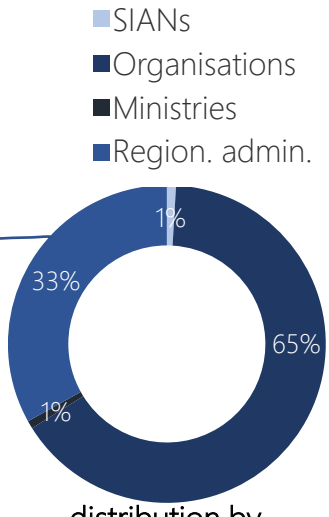
suspicious IS events detected
≈ 14 mln

critical IS events processed
≈ 78,000

cyber incidents registered
40



priority distribution



distribution by monitoring objects

DATA SOURCES

SECURITY OPERATION CENTRE
OF THE STATE CYBER PROTECTION CENTRE
UNDER THE STATE SERVICE OF SPECIAL
COMMUNICATION AND INFORMATION PROTECTION

KEY SOURCES OF DATA COLLECTION AND CONTEXT ENRICHMENT

INTERNAL SOURCES OF CYBER THREAT DATA	9%			15%	EXTERNAL SOURCES OF CYBER THREAT DATA
USER WORKSTATION DATA	4%			6%	SERVER STATION DATA
VULNERABILITY SCANNERS	17%			5%	WEB & EMAIL TRAFFIC
NETWORK BEHAVIOR ANALYSIS DATA	6%			11%	NETWORK THREAT ANALYSIS DATA
INTRUSION DETECTION SYSTEM DATA	18%			9%	INTRUSION PREVENTION SYSTEM DATA

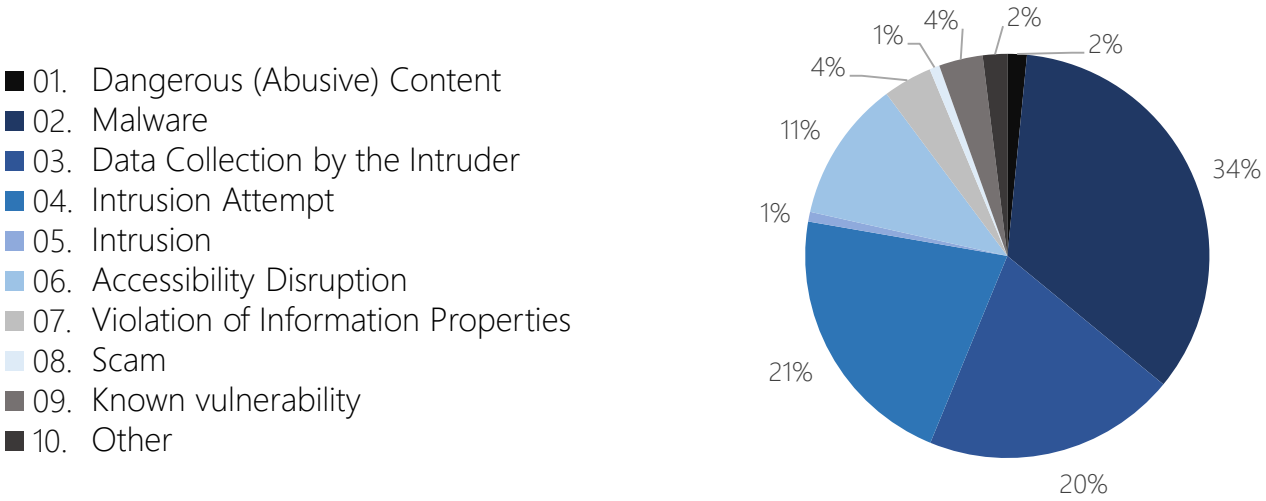
STATISTICS

SECURITY OPERATION CENTRE
OF THE STATE CYBER PROTECTION CENTRE
UNDER THE STATE SERVICE OF SPECIAL
COMMUNICATION AND INFORMATION PROTECTION

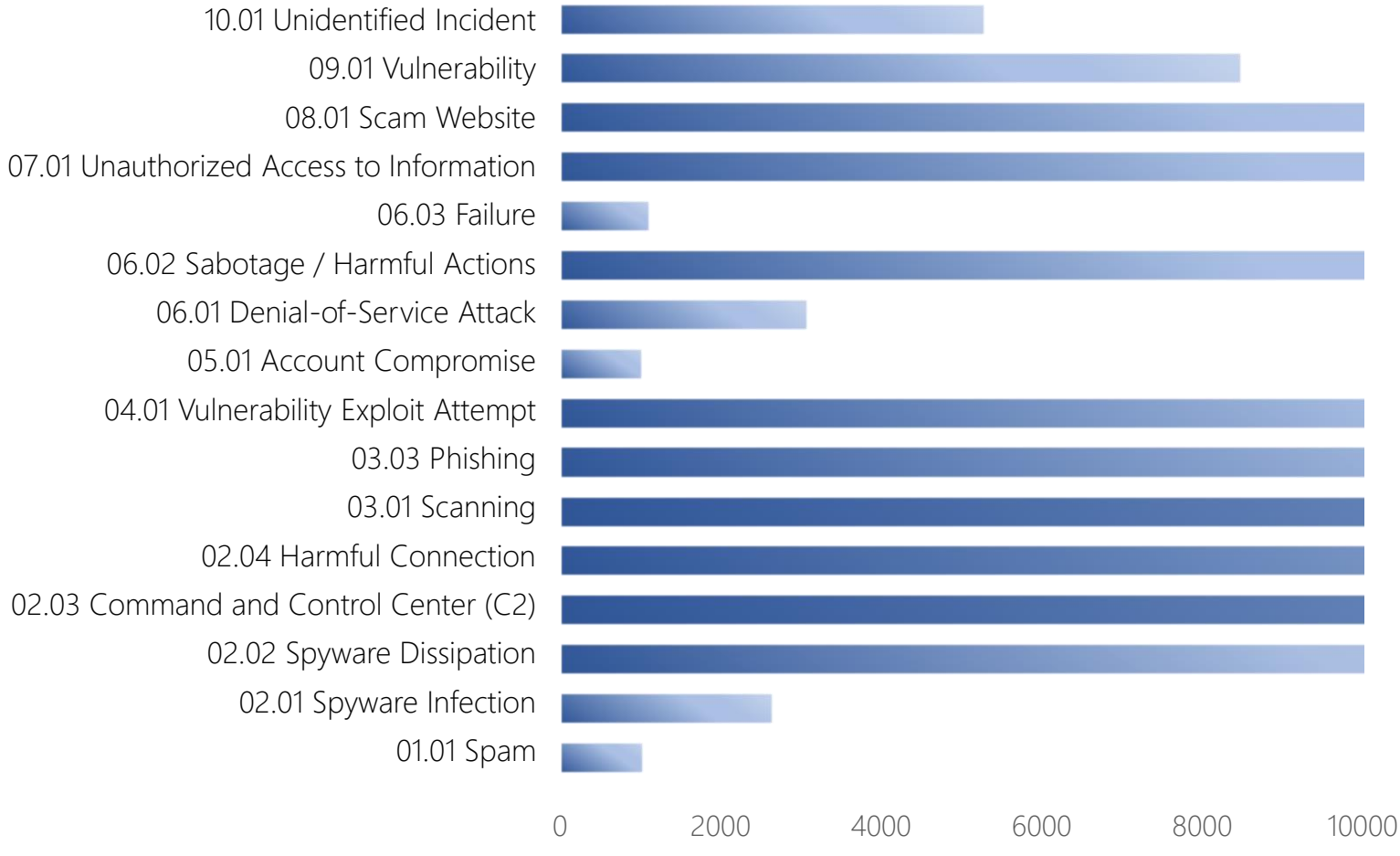
COLLECTED AND PROCESSED DATA STATISTICS

Presented as per Cyber Incident Category List, approved by the National Coordination Center for Cybersecurity under the National Security and Defense Council of Ukraine (NSDCU National Coordination Center for Cybersecurity Meeting Minutes No. 18 of 25.10.2021 (of 28.10.2021 No. 16/320/21dsk))

IS EVENT CATEGORIES



IS EVENT TYPES



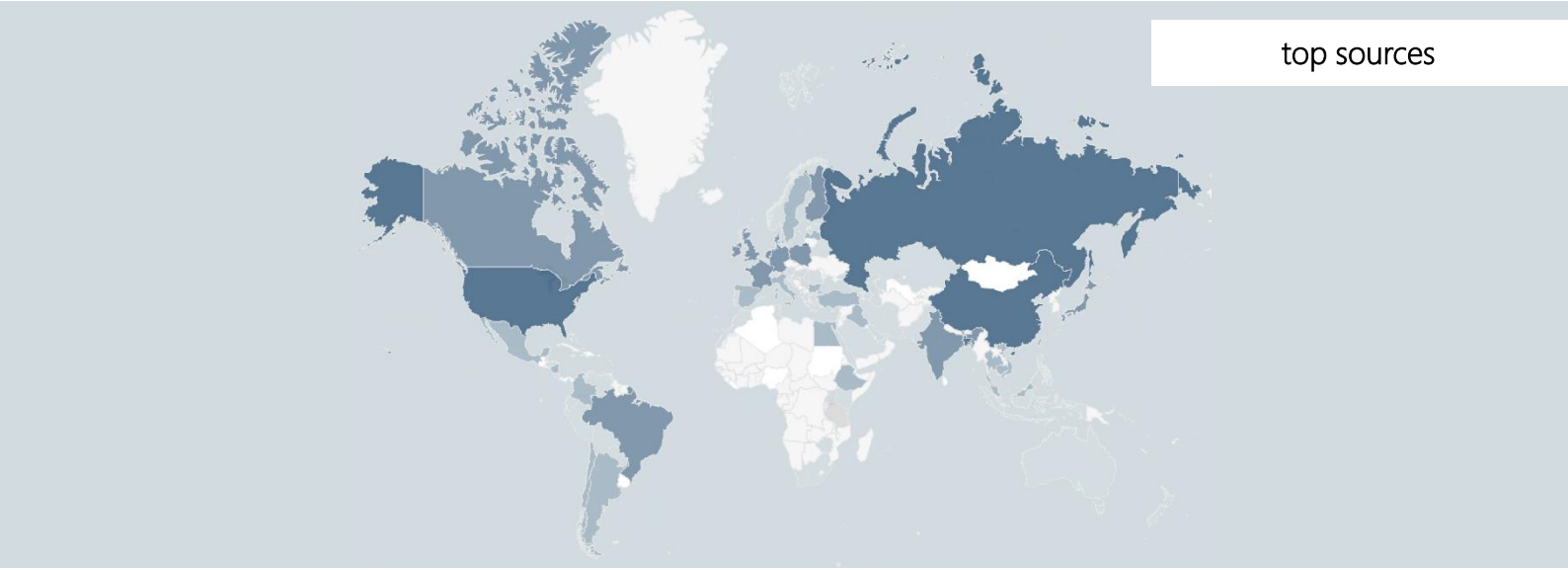
STATISTICS

SECURITY OPERATION CENTRE
OF THE STATE CYBER PROTECTION CENTRE
UNDER THE STATE SERVICE OF SPECIAL
COMMUNICATION AND INFORMATION PROTECTION

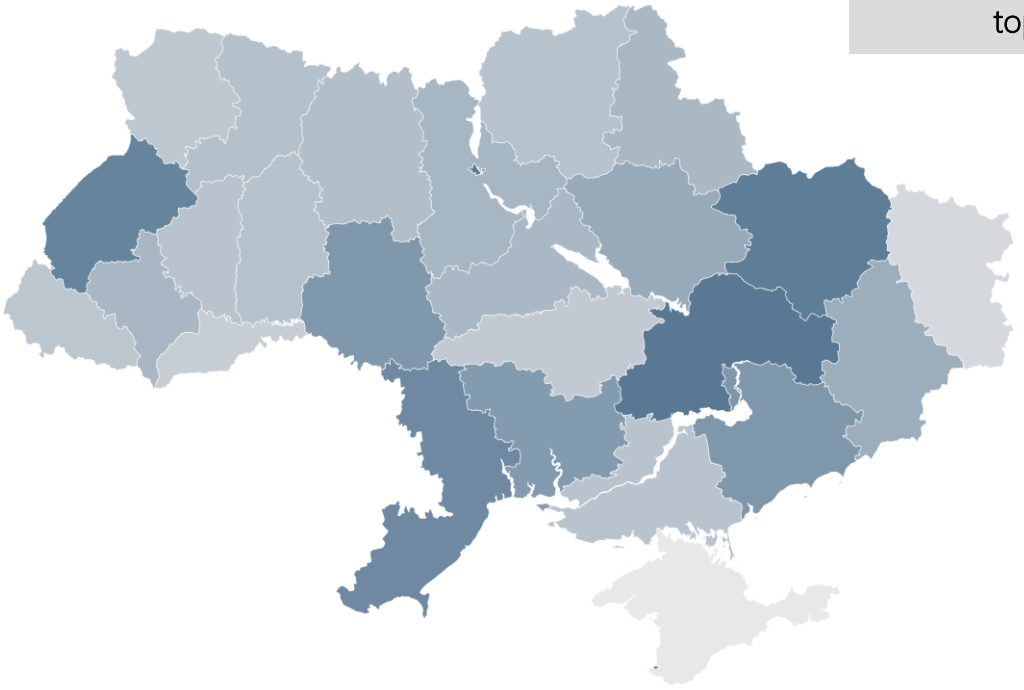
PREVALENCE OF DETECTED CRITICAL INFORMATION SECURITY EVENTS

based on the number of positives, targeting Ukrainian regions from other countries' IP addresses
(IP location in a country's delegation range does not necessarily mean that the cyberattack is attributed to this country)

top sources

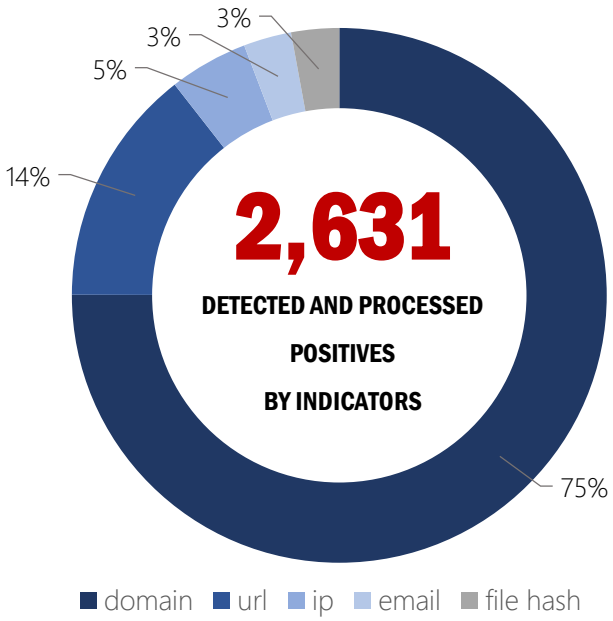


top targets

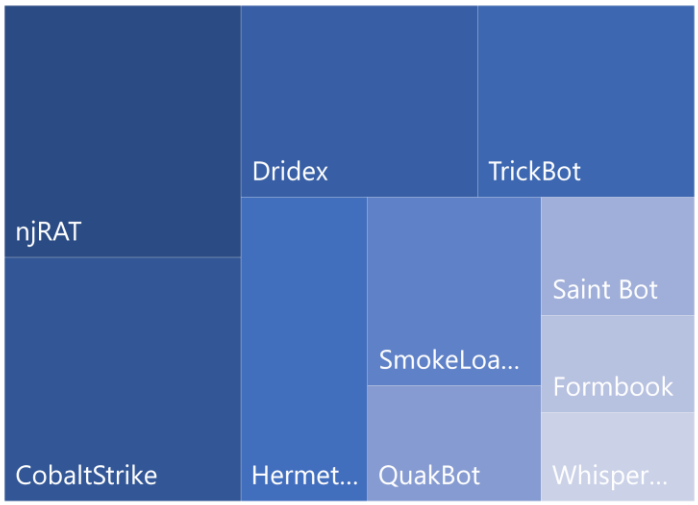


TI

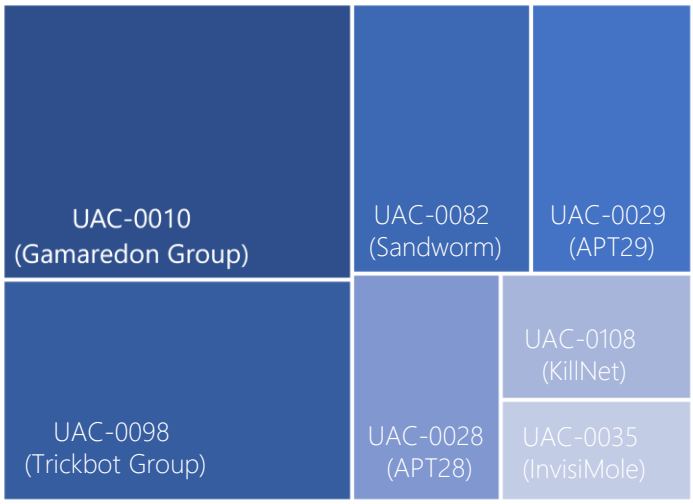
SECURITY OPERATION CENTRE
OF THE STATE CYBER PROTECTION CENTRE
UNDER THE STATE SERVICE OF SPECIAL
COMMUNICATION AND INFORMATION PROTECTION



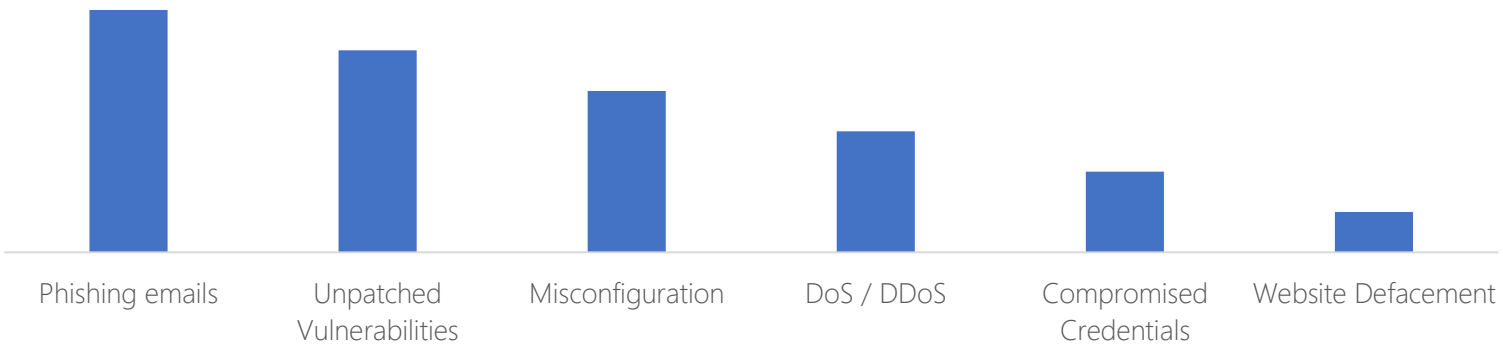
Actual Malware



Actual Hacker Groups



Popular Attack Vectors



RECOMMENDATIONS

SECURITY OPERATION CENTRE
OF THE STATE CYBER PROTECTION CENTRE
UNDER THE STATE SERVICE OF SPECIAL
COMMUNICATION AND INFORMATION PROTECTION

For the purpose of prevention and effect mitigation of popular cyberattack vectors, considering the most targeted cybersecurity sectors, we recommend taking the following actions to improve cyber defense:

ENDPOINT SECURITY

- ✓ use up-to-date licensed anti-virus software, set up regular virus checks,
- ✓ ensure timely installation (patching) of security updates for the operation system, network browsers and applications,
- ✓ perform regular backups and store backup data in separate data storages, while checking possibility of backup recovery every now and then,
- ✓ apply the Principle of Least Privilege, which means providing the least necessary access rights.

NETWORK SECURITY

- ✓ segment the network,
- ✓ ensure secure access to resources, for authorized users and devices only through implementation of the NAC (Network Access Control) principles,
- ✓ use up-to-date technologies and means for monitoring and defense from cyberattacks,
- ✓ manage user access rights through implementation of the IAM (Identity and Access Management) principles,
- ✓ prevent, detect and eliminate vulnerabilities that enable unauthorized access to the network infrastructure.

USER ACCOUNT SECURITY

- ✓ use authentication services only by trusted third-party identity providers,
- ✓ set up multi-factor authentication (MFA),
- ✓ limit the number of failed authentication attempts,
- ✓ use passwords of sufficient length and complexity, change them periodically, and do not use the same password for multiple websites / services,
- ✓ ensure safe storage of authentication data.

LEGAL FRAMEWORK

- The Law of Ukraine "On the Key Principles of Ensuring Cybersecurity of Ukraine" , which defines legal and organizational framework for ensuring protection of vital human and civil interests, social and public interests, national interests of Ukraine in cyberspace, as well as basic targets, directions and principles of national cybersecurity policy, powers of relevant government authorities, enterprises, institutions, organizations, persons and citizens; key principles for coordinating their activities to ensure cybersecurity.

- The Resolution of the Cabinet of Ministers of Ukraine of 23.12.2020 No.1295 "On Certain Issues to Ensure Functioning of the Vulnerability Detection and Cyber Incident Response System", which defines the key functioning principles of the vulnerability detection and cyber incident response system to be implemented as regards cyber defense facilities as defined in Article 4(2) of the Law of Ukraine "On the Key Principles of Ensuring Cybersecurity of Ukraine."

CONTACTS

Security Operation Centre
State Cybersecurity Center
State Service of Special Communications
and Information Protection of Ukraine

83B Yu. Illienka St., Kyiv, 04119 Ukraine
e-mail: soc@scpc.gov.ua
phone: +38 (044) 281 87 37