NAECCS | NATIONAL AUTHORITY ON ELECTRONIC CERTIFICATION AND CYBER SECURITY

ANNUAL REPORT

2022

St."Papa Gjon Pali II", No. 3, I
Floor, Tirana, Albania

Summary

1. Directorate of Electronic Certification and Control

1.1 Accrediation and Policy Sector

During 2022 the accreditation and policy sector has accomplished the following tasks:

1. In the framework of the country's integration into the European Union work has continued to update the current legal basis, including Law no. 9880/2008 "On Electronic Signature", Law no. 107/2015 "On Electronic Identification and Trusted Services", as well as Law No.2/2017 "On Cyber Security" in full harmonization with European Regulation EIDA no. 910/2014 “On Electronic Identification and Trusted Services for Electronic Transactions in the Internal Market”, as well as in full harmonization with the 2016/1148 Directive of the European Parliament and the Council “concerning measures for a high common level of the security of networks and information systems across the Union ”(NIS Directive).

   Regarding the performance of two draft laws, the draft law “On electronic identification and trusted services” and the accompanying package was issued for public consultation on 07.12.2022, a process which was completed on 10.01.2023. The draft law is being reviewed on the basis of comments brought by interested institutions and entities. The deadline for submission of this draft law is planned on the first quarter of 2023.

   For the draft law "On Cyber Security" the final proposal of the draft law was adopted, but with the approval and changes that derive from the NIS2 Directive in December 2022, in order to include some elements of this directive, this draft law was reviewed. Regarding the progress of this draft, NAECCS is preparing the full package to continue with the relevant public consultation procedures. The planned deadline for submitting this draft law is the first quarter of 2023.

2. In the context of the obligations set forth in the legislation on the declaration of assets and the prevention of conflict of interest, it has been periodically and annually reported to The High Inspectorate for the Declaration and Audit of Assets and Conflicts of Interest (“HIDAACI”).

3. During 2022 has been approved:

- “Regulation on the content and manner of documenting cyber security measures” - approved by order of the General Director no. 10, dated 14.02.2022.
- “Methodology for identifying and classifying critical infrastructures and important information infrastructures ”, approved by order of General Director No.9, dated 14.02.2022.
- Decision of Council of Ministers (“DCM”) no. 553, dated 15.7.2020 “On the approval of the list of critical information infrastructures and the list of important information infrastructures”, amended by DCM no. 761, dated 12.12.2022.
- Contribution to the process of identifying critical information infrastructures and important information infrastructures (part of the working group).

4. Contributing with continuous information and reporting on the progress of the implementation of the measures and activities provided for in the Action Plan 2021-2023 of the “Inter-Sector Strategy of the Fight against Terrorism 2021-2025”.
5. Contribution to the drafting of the strategic document in the field of prevention and opposition of violent extremism of the "New Strategy for the Prevention and Opposition of violent extremism 2022-2026.”
6. In the context of integration into the European Union a contribution was made to these areas:

- Reporting on Chapters 3, 10, 24 within GNPIE;
- Participation in meetings in the context of GNPIE;
- Completion and reporting on PPAP and PKIE 2022-2024; PKIE 2023-2025;

7. Participation in training for enhancing technical and professional capacity in the field of trusted services and cyber security organized by FESA, ENISA, etj.
8. Participation in the Conference "Speakers at Montenegro", CCB Conference, 9 May 2022 (part of the panel as a speaker and reporter).
9. Participation in the workshop "CRDF Global Cross Cyber Drill" - 7 July and 8 July 2022 "; TAIEX Expert Mission on Request for Transposition of Regulatory Framework In Cyber Security with NIS directive, 20.07.2022, Workshop "The Implementation of EU CyberseCurity Law" 14-15 December, EGAG.
10. Drafting legal reports as well as various written correspondence with institutions as needed.

1.2 Communication and Information Distribution Sector

1.2.1 Monitoring of “National Cyber Security Strategy 2020-2025”

The National Cyber Security Strategy 2020-2025 was adopted by Decision no. 1034 dated 24.12.2020, of the Council of Ministers and constitutes a key instrument for enhancing the safety of networks and information systems at national level and priority of the Albanian government.

With the contribution of the involved actors the first strategy monitoring report was drafted, which aims to evaluate the progress of implementing this strategy according to the four goals of the respective policies and objectives for the period January - December 2021.

The action plan of the National Strategy for Cyber Security 2020-2025 includes a total of 125 basic activities to be implemented during the years of adpotion of the strategy. Out of these 52% (65 activities) were fully fullfiled during the first year of 2021, while 42% (52 activities) are expected to start implementing along 2022 and onwards.

In particular, there is progress in fulfilling the purpose of the first policy on "guaranteeing cyber security at the national level, through the protection of information infrastructures, by strengthening technological and legal means" considering the fullfiled activities that are in process.

In achieving the objectives of this policy 49 Activities (39%) are foreseen, 29 of which are fully accomplished and 8 are in the process of completion as seen in the graph below:

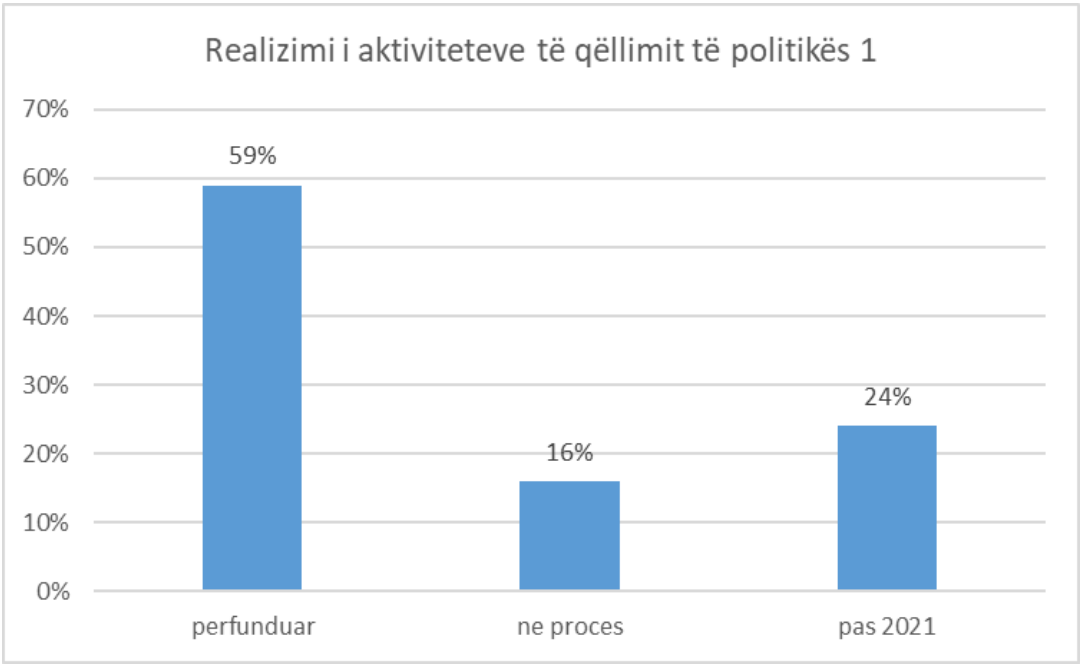


Figure 1 Fulfillment of Activities of the Purpose of the Policy 1

In meeting the objectives of the goal of the second policy, there are 19 activities (15%), 8 of which are fully achieved and 11 not yet started as seen in the graph.

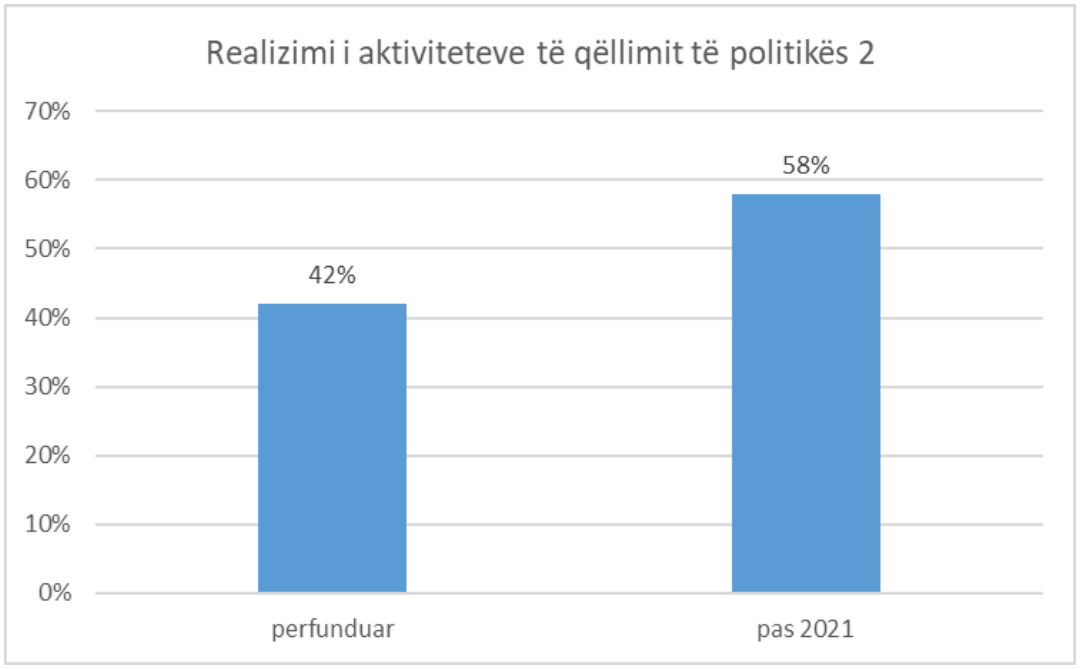


Figure 2 Fulfillment of Activities of the Purpose of the Policy 2

In meeting the objectives of the goal of the third policy, 42 activities (34%) are foreseen, 17 of which are fully realized and 25 unfented as seen in the graph.

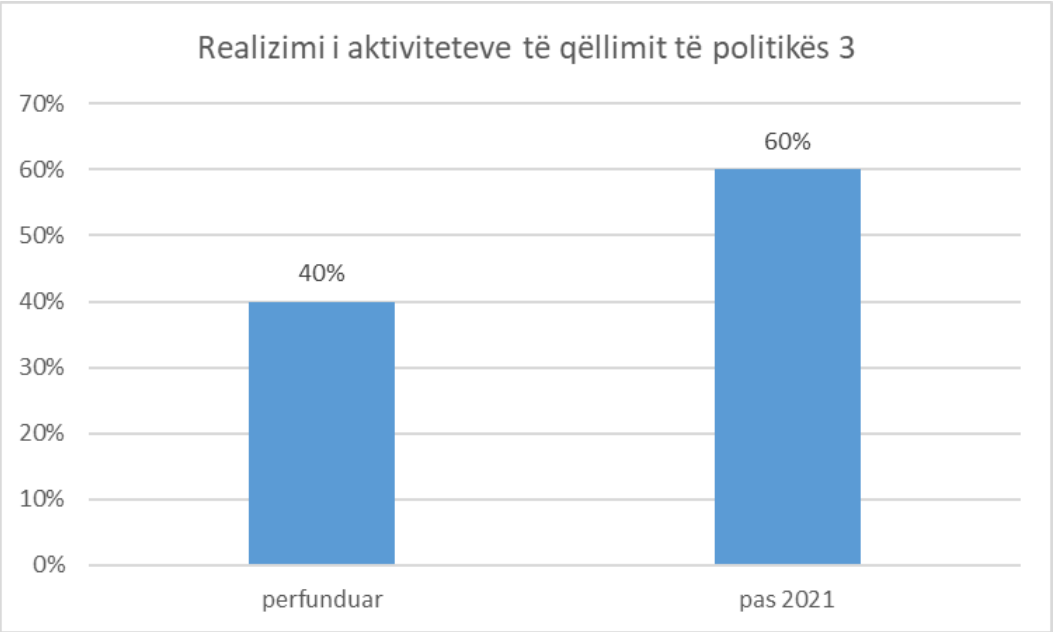


Figure 3 Fulfillment of Activities of the Purpose of the Policy 3

In meeting the objectives of the goal of the fourth policy, 15 activities (12%) are foreseen, 11 of which are fully realized and 4 unfented as seen in the graph.

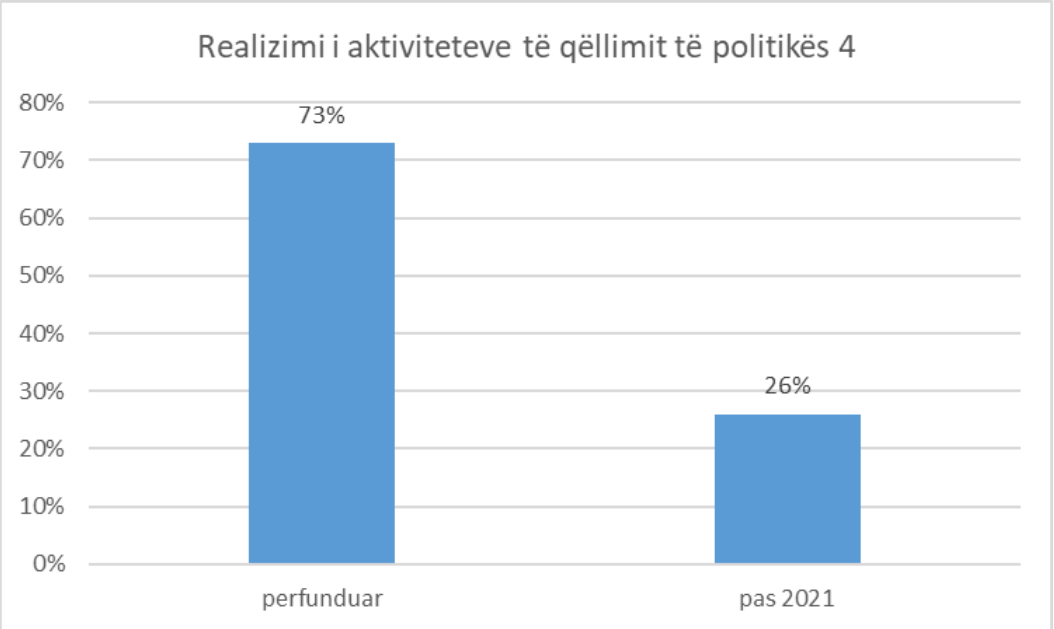


Figure 4 Fulfillment of Activities of the Purpose of the Policy 4

The full monitoring Report is found on the NAECCS official Website: https://cesk.gov.al/Publikime/2022/Monitorimi i strategjise sigurise kibernetike 2021.pdf

1.2.2 Activities to raise awareness

The communication and information distribution sector has participated in the coordination of work for the fullfilment of activities within the joint project with UNICEF Albania "Development of the mechanisms needed for online saftey of children and young people in Albania" during February - September 2022.

The results of this project are:

- ✓ Drafting of 6 documents, in the form of inter-institutional protocol, guide, analyzing report.
- ✓ 518 trained parents and teachers in 12 units / cities of Albania: Babrru, Vorë, Kavajë, Dibër, Klos, Kukës, Has, Laknas, Burrel, Bulqizë, Fushe Arrëz, Pukë, Vau Dejës, Shkodër, Tropojë, Kamëz dhe Paskuqan.
- ✓ 1 Awareness Manual drafted for parents and educators, with children's protection tips online, focusing on online trafficking.

Drafted documents are:

- Report on analyzing and identifying illegal content reporting mechanisms.
- Inter -institutional protocol for cooperation between law enforcement agencies, internet service providers and NAECCS.
- Report on analyzing and identifying the legal gap of protection of children online from sexual abuse, including the necessary recommendations.
- Report on analyzing the technical functionalities of the portal for blocking pages with illegal content, along with recommendations for improving functionalities in order to increase efficiency.
- Report on analyzing existing initiatives of Internet service providers for online child protection.
- Instruction for Internet Watching Foundation Hash List on the services of Internet Service providers.

In addition, the sector of communication and information distribution has participated in the coordination and implementation of the work for the realization of activities in the framework of piloting of the global project with the International Telecommunication Union "Creating a safe and empowering digital environment for children" for the period January-December 2022.

The results of this project are:

- ✓ Drafting of 2 awareness manuals:
    - Child-friendly manual dedicated to the protection of children on the Internet
    - Train of Trainers (ToT) Manual – dedicated to parents, to increase the safety of children on the Internet
- ✓ 37 trainings for children and young people, parents and educators, industry representatives
    - 12 trainings for children and young people
    - 15 trainings for parents and educators
    - 10 trainings for industry representatives

- ✓ 750 trainings participants
    - 190 children and young people
    - 460 parents and educators
    - 100 industry representatives
- ✓ 1 unified message published in physical stores and social media of Internet Service Providers.
- ✓ 1 poster with advice from the ITU Guidelines.

Capacity building activities

Regional Cyber Camp 19-21 Aprill 2021

The National Authority on Electronic Certification and Cyber Security in cooperation with Geneva Center for Security Council (DCAF), OSCE, Regional Cooperation Council (RCC), American Chamber of Commerce in Albania, Albanian Microfinance Association, One Telecommunications organized the innovative event on April 19-21 "Regional Cyber Camp Albania" in the premises of the Movenpick Hotel, Lalzi Bay. The purpose of the event was to develop practical skills for cooperation and information exchange between the CSIRT, the State Police and other regional institutions responsible for cyber security, as well as to raise the capacities of young people on cyber security. During the 3 days of the activity, about 100 young people and 50 professionals from Albania, Kosovo, Serbia, Bosnia Herzegovina, North Macedonia and Montenegro deepened their knowledge and exchanged the best national practices in the field of cyber security.

CyberSec 3.0
22-23 December 2022


The National Authority on Electronic Certification and Cyber Security organized two days in a row, with all Critical Information Infrastructures divided by sector, in-depth training on "Cyber Incident Management", in fulfillment of the objectives of the "National Cyber Security Strategy 2020-2025 ". The purpose of the training is in the wake of increasing the professional capacities needed for operators of critical infrastructures in Albania, as one of the main objectives of the Authority. Also, cyber training was organized with scenarios based on best practices.


1.2.2 Promotional materials

During the year 2022, in implementation of the communication plan of the sector, the realization and publication on the social networks of the National Authority on Electronic Certification and Cyber Security of 3 promotional videos for the awareness of the community for increasing the level of cyber security, which have achieved more than 6000 views on social media.

“Creating a safe and prosperous cyber space for children”

- Video “ Children's safety on the Internet”
- Video “Tips for parents and educators about children's online safety”
- Video “Guidelines for the Child Protection Industry on the Internet”

Also, blogs, news and articles, based on the analysis of the current situation of ICT and cyber security, are periodically drawn up on the official social media communication channels of the Authority.

1.2.3 Cyber Security Bulletins

January 2022

AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Cyber Security News Bulletin

January 2022

HACKERS ARE TAKING OVER CEO ACCOUNTS WITH ROGUE OAUTH APPS

Threat analysts have observed a new campaign named 'OiVaVoii', targeting company executives and general managers with malicious OAuth apps and custom phishing lures sent from hijacked Office 365 accounts.

According to a report from Proofpoint, the campaign is still ongoing, though Microsoft is monitoring the activity and has already blocked most of the apps.

The impact of executive account takeovers ranges from lateral movement on the network and insider phishing to deploying ransomware and business email compromise incidents.

WIFI-CONNECTED SECURITY CAMERA COULD BE MANIPULATED TO SPY ON COMMUNICATIONS, AMONG OTHER MALICIOUS ACTIONS

Cisco Talos recently discovered several vulnerabilities in the Reolink RLC-410W security camera that could allow an attacker to perform several malicious actions, including performing man-in-the-middle attacks, stealing user login credentials and more.

DATA PROTECTION DAY

Your personal data is important.

In the EU, the protection of your personal data is a fundamen right.

The General Data Protection Regulation (GDPR) applies ac the EU and gives you more control over your personal data. It become the global benchmark for privacy regulation.

Increasingly, the GDPR is also becoming the foundation of digital policy on which we are building other initiatives under European Digital Strategy.

Europe is not only ensuring strong privacy rules at home, they leading the way globally.

MOST RANSOMWARE INFECTIONS ARE SELF-INSTALLED

New research from managed detection and response (MI provider Expel found that most ransomware attacks in 2 were self-installed.

Researchers found eight out of ten ransomware infecti occurred after victims unwittingly opened a zipped containing malicious code. Abuse of third-party acc accounted for 3% of all ransomware incidents, and 4% w caused by exploiting a software vulnerability on perimeter.

Most Ransomware Infections are Self-Installed - Infosecurity Magazine (infosecurity-magazine.com)

CONTACT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

February 2022

AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Cyber Security News Bulletin

February 2022

HOW TO PROTECT OUR DIGITAL ASSETS, INFRASTRUCTURE AND IDENTITIES

As Russia's attack on Ukraine escalates and because of the sanctions that EU countries are imposing, we need to be aware and vigilant about our behavior in cyberspace.

To mitigate the impact of potential attacks, National Authority for Electronic Certification and Cyber Security suggests several steps to protect our digital assets, infrastructure and identities.

Tips for organizations:
- Make sure your devices and systems are up to date
- Validate remote access for your organization
- Test back up procedures
- Interact with your organization's CSIRT team if you suspect possible attacks

For individuals:
- Implement multi-factor authentication for your accounts.
- Update equipment
- Do not click on insecure links
- Increase the complexity of passwords and implement cyber hygiene.

SAFER INTERNET DAY

Safer Internet Day (SID) is an annual celebration aiming to promote a responsible, respectful, critical and creative use of digital technologies, especially among children and young people!

INTERNATIONAL DAY OF WOMEN AND GIRLS IN SCIENCE

On 22 December 2015, the General Assembly decided to establis annual International Day to recognize the critical role women girls play in science and technology.

The International Day of Women and Girls in Science, celebrate 11 February, is implemented by UNESCO and UN-Women(li external), in collaboration institutions and civil society partners aim to promote women and girls in science. This Day i opportunity to promote full and equal access to and participati science for women and girls.

CHILD ONLINE PROTECTION #THINKCYBER

National Authority for Electronic Certification and Cyber Securi collaboration agreement with the Internati Telecommunication Union (ITU) within the context of ITU's gl programming on child online protection has developed aware videos on "How to Protect your CHILD and Be aware of what he is accessing on the Internet!".

CONTACT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

March 2022

AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Cyber Security News Bulletin

March 2022

TRACKING CYBER ACTIVITY IN EASTERN EUROPE

In early March, Google's Threat Analysis Group (TAG) published an update on the cyber activity it was tracking with regard to the war in Ukraine. Since our last update, TAG has observed a continuously growing number of threat actors using the war as a lure in phishing and malware campaigns. Government-backed actors from China, Iran, North Korea and Russia, as well as various unattributed groups, have used various Ukraine war-related themes in an effort to get targets to open malicious emails or click malicious links.

Financially motivated and criminal actors are also using current events as a means for targeting users. For example, one actor is impersonating military personnel to extort money for rescuing relatives in Ukraine. TAG has also continued to observe multiple ransomware brokers continuing to operate in a business as usual sense.

https://www.cyber security-review.com/news-march-2022/tracking-cyber-activity-in-eastern-europe/

MICROSOFT CONFIRMS IT WAS BREACHED BY HACKER GROUP

Microsoft has confirmed it was breached by the hacker group Lapsus$, adding to the cyber gang's growing list of victims.

In a blog post late Tuesday, Microsoft said Lapsus$ had compromised one of its accounts, resulting in "limited access" to company systems but not the data of any Microsoft customers."

Our cybersecurity response teams quickly engaged to remediate the compromised account and prevent further activity," Microsoft said in the post.

The disclosure comes after Lapsus$ claimed credit for compromising Okta, the widely used digital identity management firm. On Tuesday evening, following an investigation into those claims, Okta acknowledged that hundreds of its customers may have been affected by a breach in January linked to one of Okta's outside contractors.

https://www.cybersecurity-review.com/news-march-2022/microsoft-confirms-it-was-breached-by-hacker-group/

CRITICAL SECURITY PATCHES ISSUED BY MICROSOFT, ADOBE AND OTHER MAJOR SOFTWARE FIRMS

Microsoft's Patch Tuesday update for the month of March has made officially available with 71 fixes spanning across its soft products such as Windows, Office, Exchange, and Defender, an others.

Of the total 71 patches, three are rated Critical and 68 are Important in severity. While none of the vulnerabilities are liste actively exploited, three of them are publicly known at the tim release.

It's worth pointing out that Microsoft separately addressed 21 f in the Chromium-based Microsoft Edge browser earlier this mo

https://thehackernews.com/2022/03/critical-security-patches-issued-by-

FIVE TOP CYBERSECURITY TRENDS TO KEEP AN EYE ON IN 2022

Countless scams, security breaches, frauds and data leak happened last year, and the trends indicate they'll keep happe in 2022. In fact, the results of a study by PwC show compa growing concern regarding information security and that 69 organizations predict they'll increase their investments cybersecurity in 2022.

Here are five trends in cybersecurity we suggest companies kee eye on in this new year.

1. Ransomware Cyberattacks.
2. 5G Vulnerabilities
3. Remote Environments And The Decentralization Of Access
4. Synthetic Identities
5. Offline Fraud

CONTACT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

April 2022

AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Cyber Security News Bulletin

April 2022

REGIONAL CYBER CAMP ALBANIA 2022

The National Authority for Electronic Certification and Cyber Security in cooperation with the Geneva Centre for Security Council (DCAF), OSCE, Regional Cooperation Council (RCC), American Chamber of Commerce in Albania, Albanian Microfinance Association, One Telecommunications organized on April 19-21 an innovative event "Regional Cyber Camp Albania" near Moverspick Hotel, Lalzi Bay.

The event aimed to develop practical skills for cooperation and exchange of information between CSIRT's, LEA (law-enforcement agency), and other regional institutions responsible on cyber security on one side and building capacities of youth towards their education on cyber security.

During the 3 days of the event, about 100 young people and 50 professionals from Albania, Kosovo, Serbia, Bosnia and Herzegovina, Northern Macedonia and Montenegro deepened their knowledge and exchanged best national practices in the field of cyber security.

LOG4J FLAW: THOUSANDS OF APPLICATIONS ARE STILL VULNERABLE WARN SECURITY RESEARCHERS

Months on from a critical zero-day vulnerability being disclose the widely-used Java logging library Apache Log4j, a signifi number of applications and servers are still vulnerable cyberattacks because security patches haven't been applied.

First detailed in December, the vulnerability (CVE-2021-44 allows attackers to remotely execute code and gain acces systems that use Log4j.

Not only is the vulnerability relatively simple to take advantag but the ubiquitous nature of Log4j means that it's embedded vast array of applications, services and enterprise software that are written in Java – and used by organisations and individ around the world.

https://www.cybersecurity-review.com/news-april-2022/log4j-flaw-thousands-of-applications-are-still-vulnerable-warn-security-researchers/

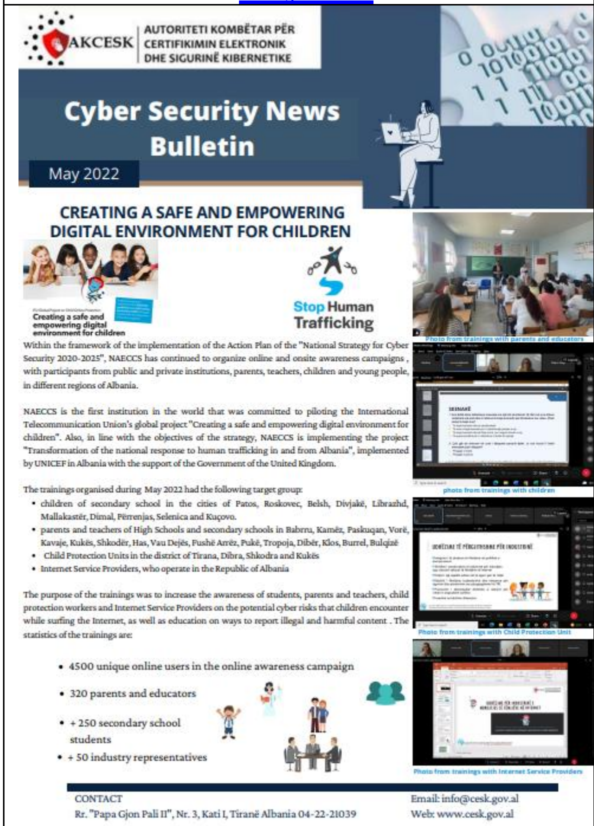
GOOGLE ISSUES THIRD EMERGENCY FIX FOR CHROME THIS YEAR

Google is issuing fixes for two vulnerabilities in its Chrome browser.

The emergency updates the company issued this week impact almost three billion users of its Chrome browser as well as t using other Chromium-based browsers, such as Microsoft E Brave and Vivaldi.

CONTACT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

May 2022



AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

AKCESK

Cyber Security News Bulletin

May 2022

CREATING A SAFE AND EMPOWERING DIGITAL ENVIRONMENT FOR CHILDREN

Within the framework of the implementation of the Action Plan of the "National Strategy for Cyber Security 2020-2025", NAECCS has continued to organize online and onsite awareness campaigns , with participants from public and private institutions, parents, teachers, children and young people, in different regions of Albania.

NAECCS is the first institution in the world that was committed to piloting the International Telecommunication Union's global project "Creating a safe and empowering digital environment for children". Also, in line with the objectives of the strategy, NAECCS is implementing the project "Transformation of the national response to human trafficking in and from Albania", implemented by UNICEF in Albania with the support of the Government of the United Kingdom.

The trainings organised during May 2022 had the following target group:

- children of secondary school in the cities of Patos, Roskovec, Belsh, Divjakë, Librazhd, Mallakastër, Dimal, Përrenjas, Selenica and Kuçovo.
- parents and teachers of High Schools and secondary schools in Babrru, Kamëz, Paskuqan, Vorë, Kavaje, Kukës, Shkodër, Has, Vau Dejës, Fushë Arrëz, Pukë, Tropoja, Dibër, Klos, Burrel, Bulqizë
- Child Protection Units in the district of Tirana, Dibra, Shkodra and Kukës
- Internet Service Providers, who operate in the Republic of Albania

The purpose of the trainings was to increase the awareness of students, parents and teachers, child protection workers and Internet Service Providers on the potential cyber risks that children encounter while surfing the Internet, as well as education on ways to report illegal and harmful content . The statistics of the trainings are:

- 4500 unique online users in the online awareness campaign
- 320 parents and educators
- + 250 secondary school students
- + 50 industry representatives

Photo from trainings with parents and educators

photo from trainings with children

Photo from trainings with Child Protection Unit

Photo from trainings with Internet Service Providers

CONTACT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I, Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

June 2022

AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

AKCESK

Cyber Security News Bulletin

June 2022

Congress Declares June 2022 as "National Cybersecurity Education Month"

The Congress of the United States has resolved that June 2022 shall be designated as "National Cybersecurity Education month" in an effort to recognize the essential role of cybersecurity education to the NICE vision to "prepare, grow, and sustain a cybersecurity workforce that safeguards and promotes America's national security and economic prosperity." The bipartisan and bicameral resolution (House Resolution 1154 and Senate Resolution 680) was introduced in the House of Representatives and the Senate earlier this month, and agreed to by the Senate on June 15th.

At the Annual NICE Conference & Expo held in Atlanta earlier in June as part of National Cybersecurity Education Month, new CyberSeek data was announced that revealed a significant increase in the number of open jobs in cybersecurity in the United States. Several public and private sector entities continue to coordinate efforts to address the cybersecurity workforce shortage by expanding educational opportunities. Even though cybersecurity education occurs throughout the year, there are several efforts during the month of June to bring the cybersecurity education community together through conferences, workshops, teacher training, faculty development, summer camps, and more.

https://www.nist.gov/news-events/news/2022/06/recognizing-june-national-cybersecurity-education-month

Canada Introduces New Cybersecurity Legislation for Critical Infrastructure

Canada's Minister of Public Safety, Marco Mendicino, announced further steps to strengthen Canada's cybersecur with the introduction of Bill C-26, An Act Respecting Cy Security (ARCS). This proposed legislation is intended protect Canadians and bolster cybersecurity across financial, telecommunications, energy, and transportati sectors.

What Your Parents Should Know About Cybersecurity

While a cybersecurity event can be a frightening for anyo understanding how they can happen and how to avoid one make all the difference.

Give some peace of mind to Mom and Dad and your family explaining to them what they should know about cybersecu and the risks that await on the Internet, and sleep a little be yourself.

CONTACT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

July 2022

AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

AKCESK

Cyber Security News Bulletin

July 2022

New Lilith ransomware emerges with extortion site, lists first victim

A new ransomware operation has been launched under the name 'Lilith,' and it has already posted its first victim on a data leak site created to support double-extortion attacks.

Lilith is a C/C++ console-based ransomware discovered by JAMESWT and designed for 64-bit versions of Windows. Like most ransomware operations launching today, Lilith performs double-extortions attacks, which is when the threat actors steal data before encrypting devices.

According to a report by researchers at Cyble who analyzed Lilith, the new family doesn't introduce any novelties. However, it's one of the latest threats to watch out for, along with RedAlert and Omega that also recently emerged.

Ransomware attacks rose 47 percent in July

Ransomware attacks rose 47 percent from June to July, with the majority of attacks targeting the industrials sector, according to a report released on Thursday by cybersecurity firm NCC Group. Previous reports conducted by the firm indicated that ransomware cases had declined in the spring but soon picked up again, with attacks increasing from 135 in June to 198 in July.

Cyberattacks remain a great ri the global financial system

Cybersecurity in banking has become more importa as the rapid evolution of digital banking has customers finding it more convenient to manage th through online channels, exposing banks an institutions to increased levels of cyberattacks geopolitical tensions in 2022 have also contribute the rise in cyberattacks in the financial sector.

According to GlobalData estimates, the global cy industry in the retail banking sector will grow from in 2020 to $11.6 billion in 2025 at a compound an rate (CAGR) of 8.1%.

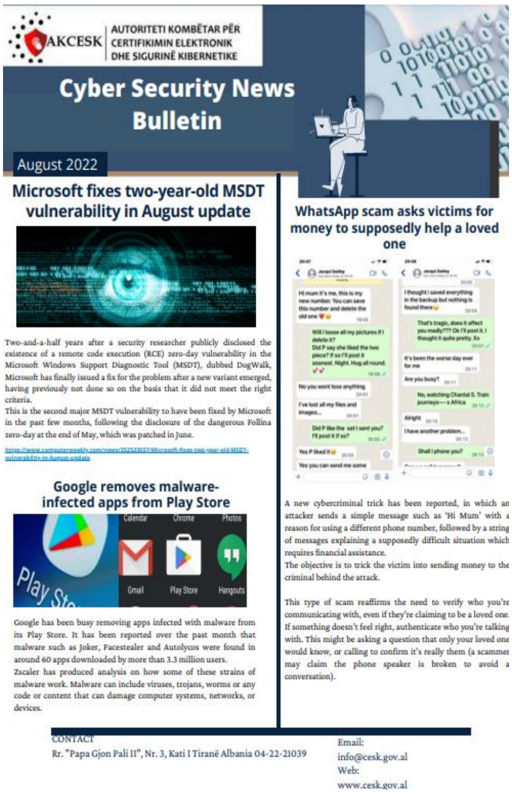
https://www.verdict.co.uk/cyberattacks-banking/

Australian Researchers Develop Cyber Honeypot Tech

A collaboration between the Cyber Security Research Centre, CSIRO's Data61 and the Austr cyber company, DecaaS is in the process of comme Those involved noted that significant benefits were the project's unique working environment; stude alongside the industry, leading to a wealth of transfer between both parties.

CONTACT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

August 2022



AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

AKCESK

Cyber Security News Bulletin

August 2022

Microsoft fixes two-year-old MSDT vulnerability in August update

Two-and-a-half years after a security researcher publicly disclosed the existence of a remote code execution (RCE) zero-day vulnerability in the Microsoft Windows Support Diagnostic Tool (MSDT), dubbed DogWalk, Microsoft has finally issued a fix for the problem after a new variant emerged, having previously not done so on the basis that it did not meet the right criteria.

This is the second major MSDT vulnerability to have been fixed by Microsoft in the past few months, following the disclosure of the dangerous Follina zero-day at the end of May, which was patched in June.

https://www.computerweekly.com/news/252523657/Microsoft-fixes-two-year-old-MSDT-vulnerability-in-August-update

Google removes malware-infected apps from Play Store

Google has been busy removing apps infected with malware from its Play Store. It has been reported over the past month that malware such as Joker, Facestealer and Autolycos were found in around 60 apps downloaded by more than 3.3 million users.

Zscaler has produced analysis on how some of these strains of malware work. Malware can include viruses, trojans, worms or any code or content that can damage computer systems, networks, or devices.

WhatsApp scam asks victims for money to supposedly help a loved one

A new cybercriminal trick has been reported, in which an attacker sends a simple message such as 'Hi Mum' with a reason for using a different phone number, followed by a string of messages explaining a supposedly difficult situation which requires financial assistance.

The objective is to trick the victim into sending money to the criminal behind the attack.

This type of scam reaffirms the need to verify who you're communicating with, even if they're claiming to be a loved one. If something doesn't feel right, authenticate who you're talking with. This might be asking a question that only your loved one would know, or calling to confirm it's really them (a scammer may claim the phone speaker is broken to avoid a conversation).

CONTACT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

September 2022

AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Cyber Security News Bulletin

September 2022

NATIONAL AUTHORITY FOR ELECTRONIC CERTIFICATION AND CYBER SECURITY PARTICIPATES IN THE EVENT : "ADVANCING THE CYBER RESILIENCE AGENDA WITH THE WESTERN BALKANS PARTNERS"

The General Director of the National Authority for Electronic Certification and Cyber Security, Ms. Vilma Tomço, participates in the event "Advancing the Cyber Resilience Agenda with The Western Balkans Partners", in Brussels.

This event, attended by officials and representatives of the Western Balkans Region, as well as EU institutions, member states and key stakeholders, had the focus at increasing cooperation by advancing a concrete agenda oriented towards EU commitments and partners in the Western Balkans.

During the discussions, participants put forward several mechanisms to address current challenges, including the establishment of POCs, closer involvement of Western Balkan partners and agencies in EU-led practical exercises, sharing of threat assessments and pursuing more cooperation tight on legal and regulatory processes for cyber security such as NIS2.

New European Union cybersecurity proposal takes aim at cybercrime

Lawmakers are seeking to strengthen cybersecurity requireme across the European Union, advancing new legislation to bol security requirements for all digital hardware and softw products.

The proposed law, titled the Cyber Resilience Act, would co everything from computers and mobile phones to smart kitc appliances and digital children's toys. The proposed legislati which was unveiled by the European Commission earlier t month, mandates that products are designed, developed produced in ways that mitigate cybersecurity risks.

https://news.sophos.com/en-us/2022/09/15/new-european-union-cybersecurit proposal-takes-aim-at-cybercrime/

Samsung says customer data stolen in July data breach

Electronics giant Samsung has confirmed a data breach affecting customers' personal information.
This is the second time Samsung has confirmed a data breach this year. In March, the company admitted that the Lapsus$ hacking group — the same group that infiltrated Nvidia, Microsoft and T-Mobile — obtained and leaked almost 200 gigabytes of confidential data, including source code for various technologies and algorithms for biometric unlock operations.

https://techcrunch.com/2022/09/02/samsung-data-breach/

Uber details how it got hacked, claims limited damage

Uber asserts the threat actor behind the last cyberattack did not access the company's production environment, any user accounts or databases it uses to store sensitive information.

The attacker did, however, gain access and exfiltrate Slack messages, data for a tool Uber's finance team uses to manage invoices, and the company's dashboard at HackerOne, where it stores vulnerability reports. The company said it took multiple protective measures in response to the attack.

https://www.cybersecurityeditor.com/news/uber-attack-details/6321933/

CONTACT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

October 2022

AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Cyber Security News Bulletin

October 2022

AKCESK PARTICIPATES IN THE CONFERENCE: "DIGITAL SOCIETIES: THE ESTONIAN EXPERIENCE IN ALBANIA"

The National Authority for CESK participated in the conference "Digital Societies: Estonian Experience in Albania". In this event, the topic was the important issue of digitization in Alban.
The conference was also attended by some of the national institutions with impact on digitalization, as well as students and other supporters of digitalization in public services and especially in the financial sector.
At this event, the National Authority for CESK presented the regulatory framework for electronic identification and trusted services, which is in line with the EU and aims to increase the safe use of public services, as well as the possibility of expanding safe services from the sector private.

AKCESK IN PARTNERSHIP WITH THE PRESENCE OF OSCE IN ALBANIA ORGANIZED THE AWARENESS CAMPAIGN ON CYBER THREATS

In the framework of October - the European Month for Cyber Security, from October 19 to November 2, 2022, AKCESK met with children, parents, teachers, psychologists and social workers in schools to raise community awareness of cyber threats.
The information sessions, held in Korça, Pogradec, Shkodër Malësi e Madhe, Krështen and Lezhë, also aimed to help young people protect themselves online, while threats to technology and confidential data become more and more common. AKCESK organized these activities in partnership with the OSCE Presence in Albania.

AKCESK continues the campaign on the Protection of Children on the Internet wit the support of the International Telecommunication Union

In the framework of October - the European Month for Cyb Security, the National Authority for CESK in cooperation wi the International Telecommunication Union has drafted t unified message regarding the Protection of Children on t Internet.
This poster shows some rules that parents should apply guide their children to surf the Internet as safely as possible.
This campaign was also supported by Internet Servi Providers in Albania, who spread the message everywhere their social media and stores.

CONTACT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Nëntor 2022

AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Cyber Security News Bulletin

November 2022

THE GENERAL DIRECTOR OF AKCESK, MR. IGLI TAFA MET WITH THE AMBASSADOR AT LARGE FOR CYBER SPACE AND DIGITAL POLICIES OF THE USA, MR. NATHANIEL FICK

The General Director of AKCESK, in the role of the National Coordinator for Cyber Security, Mr. Igli Tafa held a meeting with the Ambassador at Large for Cyberspace and Digital Policy of the USA, Mr. Nathaniel Fick.
The meeting took place in the framework of the commitments of the Albanian government, to strengthen alliances with strategic partners, in order to increase the level of Cyber Security in the country.
Ambassador Fick expressed the readiness of the United States of America to support Albania as its ally, in increasing capacities in the function of cyber defense, as well as in strengthening cooperation in this field.
Also, Mr. Tafa assured Ambassador Fick of fulfilling the commitments as a country of the Euro-Atlantic Alliance, taking the necessary measures to create a safe cyber ecosystem in Albania.
After the meeting, Ambassador Fick also visited the premises of the National Authority for Electronic Certification and Cyber Security.

INCREASING INSTITUTIONAL INTERACTION PRIORITY IN RAISING THE LEVEL OF CYBER SECURITY IN THE COUNTRY!

The General Director of AKCESK, in the role of the Nation Coordinator for Cyber Security, considered the issues institutional interaction and other issues related to cyb security, a priority for the creation of a safe national cyb environment, today during the meeting with hig representatives from defense and security institutions.
AKCESK, in the role of the responsible authority, is alwa available to facilitate any process related to the identification critical information infrastructures, increasing the capacities structures responsible for security, and implementing cyb security measures for these infrastructures.
The goal of creating a secure cyber ecosystem in the count starts precisely from the institutional interaction!

CYBER SECURITY IN THE BANK SECTOR, IN THE FOCUS OF AKCESK

Within the current developments in the field of cyber security, the General Director AKCESK Mr. Igli Tafa, on November 23, held the meeting on "Cybersecurity in t banking sector".
This meeting was attended by the highest security leaders in this sector. Mr. Ta revealed the new vision of AKCESK under his leadership, placing the banking sector one of the priorities with the greatest impact on information security.
This is a service within the primary commitments of the Albanian Government guarantee the financial data of citizens and the banking sector as a whole.
High-level security measures and the establishment of the cyber security operation center, were the main topics of discussion at this meeting, as an important step f increasing the level of cyber security.
Representatives of the banking sector expressed their willingness to support AKCESK.

CONTACT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Dhjetor 2022

AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Cyber Security News Bulletin

December 2022

CYBER SECURITY, A NATIONAL PRIORITY!

The general director of NAECCS Mr. Igli Tafa, following the meetings aimed at increasing the level of security and cooperation, held a meeting with the "health sector, microfinance and insurance companies" on December 7.

The purpose of this meeting was the current situation of cyber security, the possibility of increased cooperation to increase security in critical infrastructures, within the framework of the implementation of the new strategy and vision for cyber security.

The meeting discussed the change of the legal framework, with the aim of transposing European directives in the field, which brings innovation in the creation of sectoral CSIRTs and new schemes for cyber security certification for ICT equipment, products and processes.

https://cesk.gov.al/Publikime/2022/lajme.pdf

"FINANCIAL INFORMATION SECURITY, CURRENT PRIORITY OF NAECCS"

The General Director of NAECCS, at the same time the National Coordinator for cyber security Mr. Igli Tafa, held the meeting on the topic "Security of financial information, the current priority of NAECCS", with participants from the highest security managers in the banking and financial sectors.

The purpose of the meeting was to address the need to apply additional measures for the protection and provision of citizens' financial information, as a focus of the Albanian Government and a current priority of NAECCS.

https://cesk.gov.al/2022/Siguria%20e%20informacionit%20financiar.pdf

INCREASED ACTIVITIES BY THE IRANIAN APT, CALLS FOR INCREASED VIGILANCE!

An increase in activity by the Iranian APT has been noted recently. After the cyber attacks discovered on July 17, 2022, Albania became the first country in the world to cut off diplomatic relations due to a cyber attack!
At that time, specialized domestic agencies and international strategic partners addressed and assisted in the handling of the sophisticated attack, orchestrated by actors sponsored by the Islamic Republic of Iran.

https://cesk.gov.al/Publikime/2022/Lajmi%20APT.pdf

CYBER INCIDENT MANAGEMENT - REQUIRED PROCEDURE FOR CRITICAL INFRASTRUCTURES

The National Authority for Electronic Certification and Cyber Security organized two days in a row, with all Critical Information Infrastructures divided by sector, training on "Cyber Incident Management", in fulfillment of the objectives of the "National Strategy for Cyber Security 2020-2025 ".

The purpose of the training is in the wake of increasing the professional capacities needed for operators of critical infrastructures in Albania, as one of the main objectives of the Authority. Also, the training was organized with scenarios based on best practices.

"CYBER SECURITY IN THE WESTERN BALKANS IN FOCUS OF THE EU SUMMIT IN TIRANA"

Cyber security, dealing with cyber threats and hybrid threats are the areas where the EU will further deepen cross-sectoral cooperation with the Western Balkans. The summit confirmed that the EU is ready to increase its support for resistance to cyber attacks in the Western Balkans and to intensify cooperation at the regional level and with international partners.

https://cesk.gov.al/Publikime/2022/EU-WB.pdf

CONTACT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al Web: www.cesk.gov.al

1.3 Control Sector

In fulfillment of functional tasks, the Control Sector during the period January-December 2022, has audited the operators of critical and important information infrastructures in relation to the implementation of minimum security, technical and organizational measures, with the (onsite) method, in accordance with the legal framework in force and international standards.

Specifically, during the year 2022, the Control Sector has audited:

⇒ **6** Operators of Critical Information Infrastructures, including Health, Financial (Banking, Microfinance), Energy sectors

⇒ **5** Operators of Important Information Infrastructures, including the Health and Financial (Insurance Market) sectors

During the audits carried out at operators of critical infrastructures and operators of important information infrastructures, the implementation of the following organizational and technical measures was checked:

Organizational Measures

- Security policy
- Risk Management
- Organisational Security
- Security requirements for third parties
- Security of human resources and access of persons
- Asset Management
- Security events and cyber security incident management
- Work continuity management
- Information security management
- Control and Audit

Technical Measures

- Physical Security
- Access authorization management
- Cryptographic Devices
- Cyber security event detection
- Cybersecurity event tracking and assessment tools
- Protection of the integrity of communication networks
- User identity verification
- Activity of administrators and users
- Application security
- Security of industrial systems

1.3.1 Audit of Qualified Trusted Service Providers

In fulfillment of its functional duties, the Control Sector during 2022 supervised the activity of the Qualified Trusted Service Provider (ALEAT), inspecting the application offices for the device with qualified electronic certificates in accordance with the relevant legal framework**.**

In total, 12 Districts were inspected, as follows:

1. Tiranë
2. Berat
3. Dibër
4. Durrës
5. Elbasan
6. Korçë
7. Fier
8. Gjirokastër
9. Kukës
10. Lezhë
11. Shkodër
12. Vlorë

Qualified Trusted Service Providers have the legal obligation to periodically report on their activity to NAECCS.

OTSP ALEAT

During the period **January-December** 2022, Aleat has provided qualified electronic certificates to a total of **338,181** citizens in ID cards, as well as canceled about 69,370 qualified electronic certificates.

Since the launch of the service in 2016, until December 2022, approximately 301,330,654 secure electronic transactions have been carried out using electronic identification and signatures.

OTSP NAIS

During the period January-December 2022**,** QTSP NAIS has issued:
8499 Electronic certificates with electronic signature for Public Administration
15943 Electronic certificates with electronic signature for Private Entities
3512 Electronic certificates for the e-prescription system
101 599 Electronic Certificate for the fiscalization project for private production entities
1173 Electronic certificates for the fiscalization project for state production institutions
120 Electronic seals for public administration

1.3.2 Security assessment through emergency cyber security measures

The Control Sector has carried out the security assessment through emergency measures in all critical information infrastructures and important information infrastructures approved in DCM no. 553 date 15.07.2020.
They are evaluated in total:

⇒ **42** operators of critical information infrastructures.
⇒ **29** operators of important information infrastructures.

The security assesment through emergency security measures was based on the following indicators:

1. Licensing of critical/important systems, network equipment and end devices
2. The use of End of Life systems (EOL)
3. Using systems with old firmware
4. Use of the licensed central system for managing updates (patches) of the operating system
5. Use of the licensed central system for managing Antivirus updates (patches)
6. Identifying and defining the full administrator on critical/important systems
7. The use of the central system for continuous monitoring of the network (Central heuristic traffic analysis)
8. Performing filtering and monitoring of network traffic between applications and the Internet (Web Application Firewall)
9. Performing remote access analysis of devices with critical/important systems/networks
10. Backup of critical/important systems for business continuity

1.3.3 Cyber security risk assessment

Throughout the year 2022, the cyber security risk assessment was carried out for security and defense institutions, namely for:

1. Ministry of Defense
2. General Directorate of the State Police
3. Police Supervision Agency
4. Directorate of Classified Information Security
5. The High Judicial Council
6. The High Prosecutorial Council
7. The Parliament
8. Institution of the President of the Republic of Albania
9. High Inspectorate of Declaration and Control of Assets and Conflict of Interest
10. General Prosecutor's Office

1.3.4 Drafting of the new legal framework

Throughout 2022, the Control Sector has contributed to the drafting of the legal framework "On electronic identification and trusted services", transposed by the EU regulation eIDAS 910/2014, as well as the legal framework "On cyber security" transposed by the EU NIS directive 1 and NIS 2.

2. Directorate of AL-CSIRT

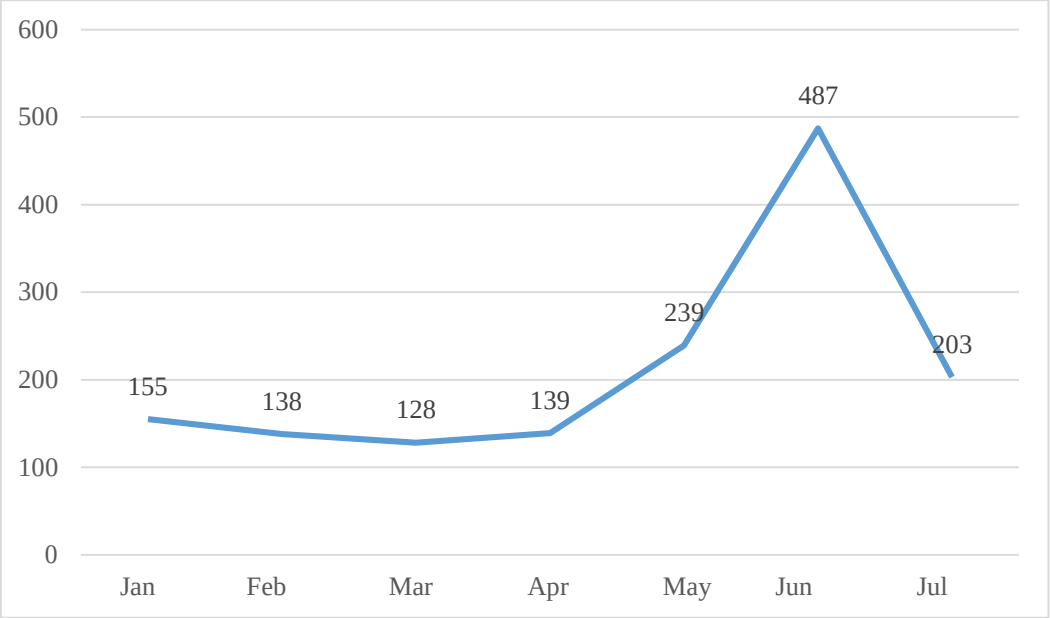
2.1 Cyber incident monitoring sector

1. Identification and classification of critical and important information infrastructures based on Law 2/2017 "On Cyber Security" Article 6, and the revision of DCM no. 553, dated 20.07.2020. The identification and classification is done based on the following sectors (Cooperation).:
   - Energy Sector: 14 Critical Information Infrastructure and 13 Important Information Infrastructures
   - Transport Sector: 31 Critical Information Infrastructure and 6 Important Information Infrastructures
   - Banking Sector: 20 Critical Information Infrastructure and 52 Important Information Infrastructure
   - Health Sector: 17 Critical Information Infrastructure and 8 Important Information Infrastructures
   - Water supply: 6 Critical Information Infrastructure and 44 Important Information Infrastructure
   - Digital Infrastructure: 54 Critical Information Infrastructure and 25 Important Information Infrastructures

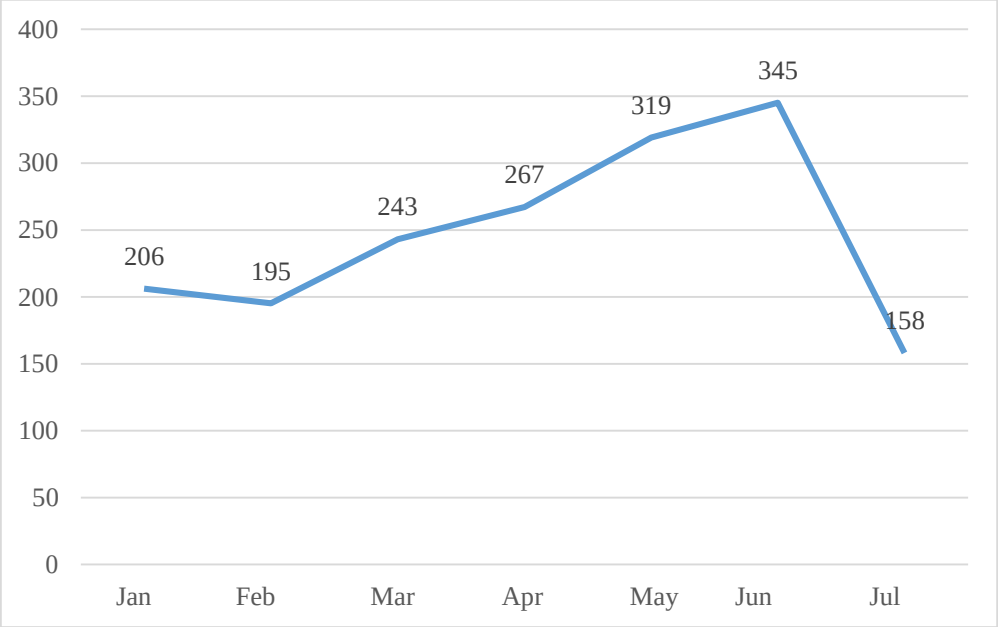
2. In accordance and fullfilment of DCM no. 141, dated 22.02.2017, NAECCS administers and maintains the unique online system for the publication of websites with illegal content, has provided support for institutions, for accessing the Online Portal. The State Agency for the Protection of Children's Rights during 2022 has reported on the Online Portal 25 pages with illegal content that have been recorded on social networks and YouTube.

3. Monitoring of some state institutions and Internet Service Providers operating in Albania, which generate malware with a source in Albania and destination in different countries, through the information coming from the Shadow Server. The processing of the data extracted from this monitoring as well as the drafting of the report. Below are the corresponding graphs for each institution and ISP expressing them as institution 1 and institution 2, also ISPs with, ISP 1 etc..

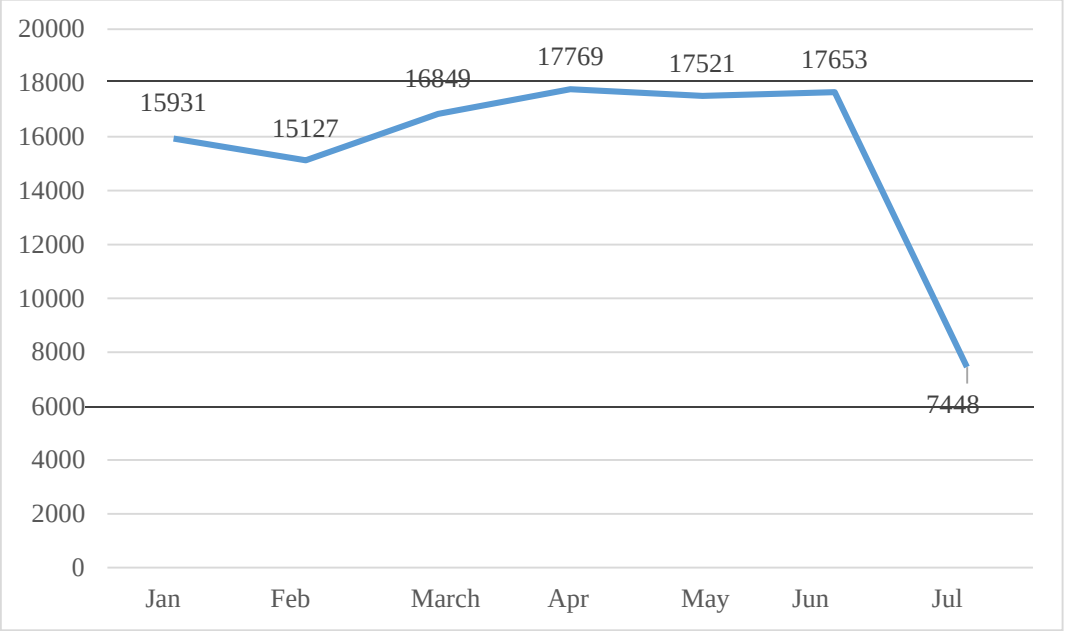
Institution -1



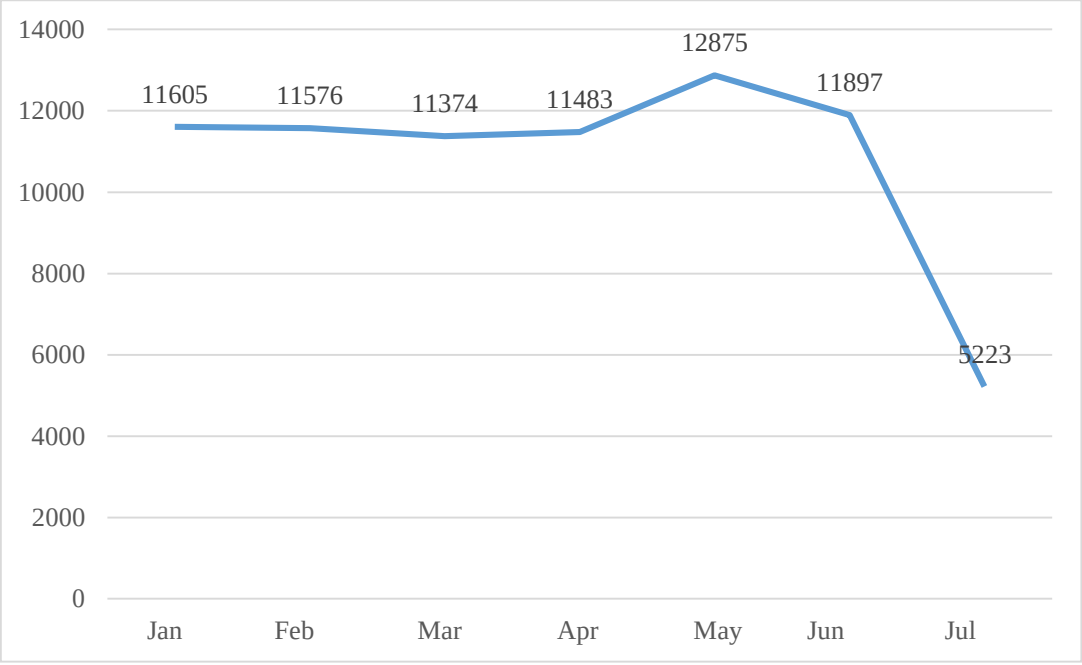
Institution -2



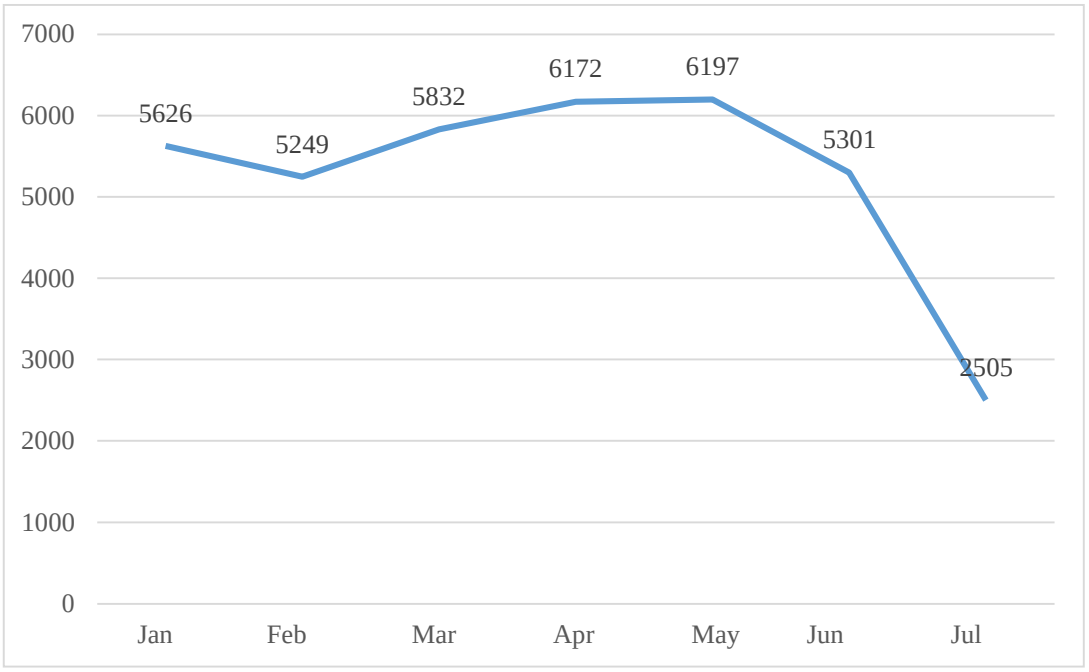
ISP -1


20000
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
15931
15127
16849
17769
17521
17653
7448
Jan
Feb
March
Apr
May
Jun
Jul

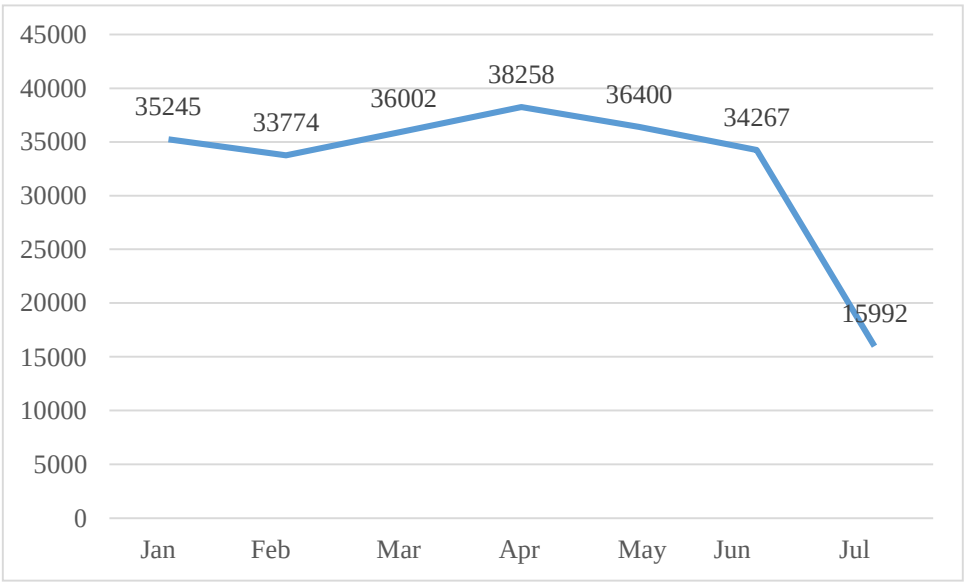
ISP -2


14000
12000
10000
8000
6000
4000
2000
0
11605
11576
11374
11483
12875
11897
5223
Jan
Feb
Mar
Apr
May
Jun
Jul

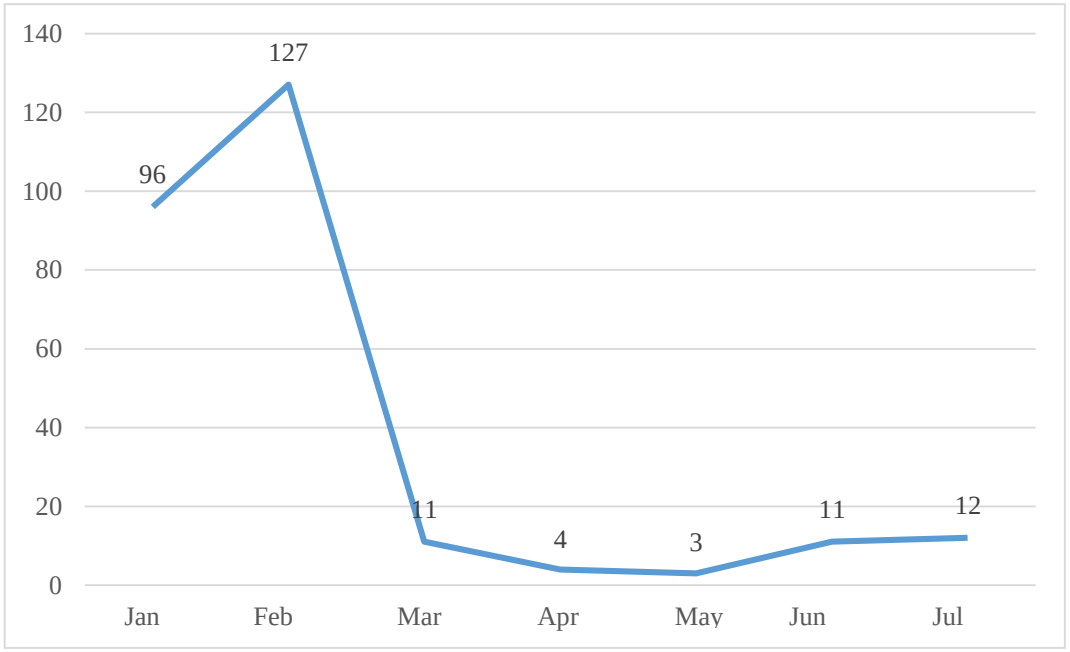
ISP -3


7000
6000
5000
4000
3000
2000
1000
0
5626
5249
5832
6172
6197
5301
2505
Jan
Feb
Mar
Apr
May
Jun
Jul

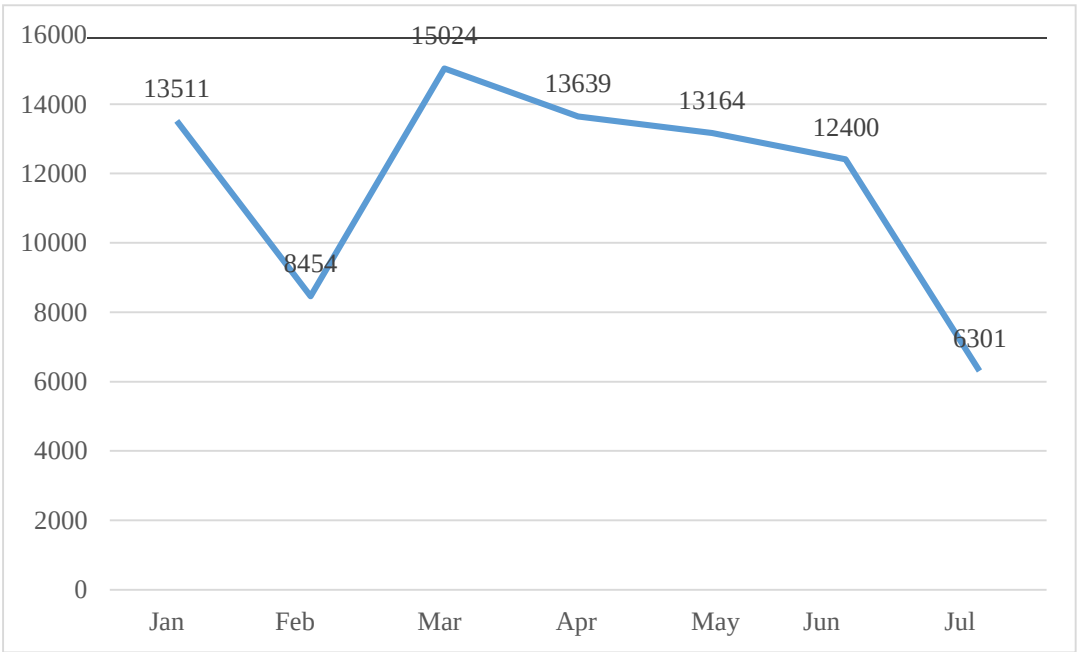
ISP -4


45000
40000
35000
30000
25000
20000
15000
10000
5000
0
35245
33774
36002
38258
36400
34267
15992
Jan
Feb
Mar
Apr
May
Jun
Jul

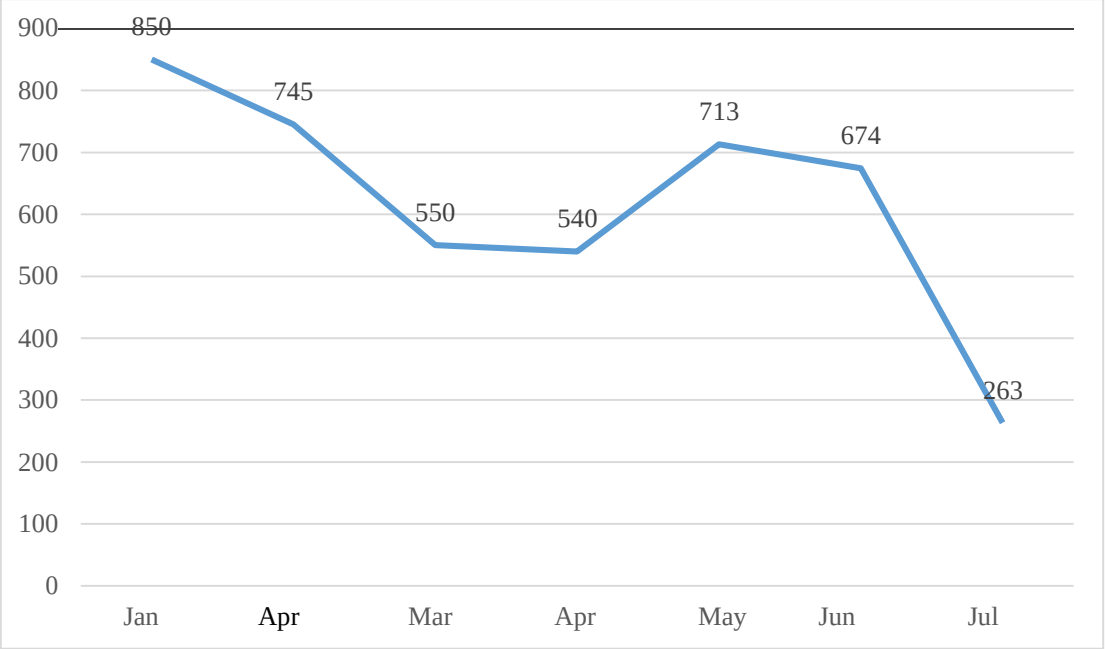
ISP -5


140
120
100
80
60
40
20
0
96
127
11
4
3
11
12
Jan
Feb
Mar
Apr
May
Jun
Jul

ISP -6


16000
14000
12000
10000
8000
6000
4000
2000
0
13511
8454
15024
13639
13164
12400
6301
Jan
Feb
Mar
Apr
May
Jun
Jul

ISP -7



4. In collaboration, the drafting of the law "On Cyber Security", based on the NIS Directive (EU 2016/1148) "concerning measures for a high common level of security of network and information systems across the Union".
5. Drafting of letters, reports, memos according to the institution's needs and the holder's requirements.

2.2 Cyber incident management sector

- Implementation of system monitoring on reporting and management of cyber incidents, in Critical and Important Information Technology Infrastructures.
- Coordinating work to resolve cyber security incidents with responsible operators in the field of national and international cyber security.
- Conducting ongoing research on developments in the field of cyber security and recommending security updates in case of findings of vulnerabilities.
- Testing of different Malware reported or not by CII/III using the technical capacities of the staff as well as the "Malware Analysis" System. Also, the creation of reports on the activity of these programs together with measures for the prevention and management of these activities - Periodic.
- Technical and methodical assistance on the decryption of compromised information State Police, through documents.
- Pentest analysis for OSHEE.AL, FSHU.AL, OSSH.AL, FTL.AL.

- Pentest analysis for UnionBank.
- Report NAIS incident goxml, cl.exe analysis of the attack from the available logs. A detailed report of the attack has been made, regardless of its classification as Cybercrime.
- Support for all Operators of critical and important information infrastructures about approach and access to the Cyber Incident Management System. (VPN and UsbToken, when they had problems, they were all remotely assisted).
- NAIS request for MISP virtual environments (malware sharing platforms).
- NAIS request for ARCTIC SECURITY virtual capacities (threat intelligence platforms).

Reports recently posted in the system From October 2022 - December 14, 2022. The reports are instructions, recommendations and countermeasures for recent incidents in the region and not only:

- Latest updates on ransomware targeting Europe and USA, IcedID IOCs December 5-8 2022, Trickbot IOCs December 6-11 2022, Cisa 5 new vulnerabilities. [14.12.2022]
- NAECCS in cooperation with national agencies has detected malicious activities from some IPs which may affect CII/III systems. IOCs and related recommendations are available attached. [13.12.2022]
- Report MuddyWater APT Group is back with updated TTP [12.12.2022]
- Latest Ransomware Updates Targeting Europe and USA Ransomware December 5-9, 2022 Broad Impact of Iran-Linked APT MuddyWater Briefing Description of Recent Attacks December 5-9. [12.12.2022]
- Malicious IPs spreading cyber attacks (28 November – 5 December 2022). IcedID known as BokBot malware. Notice about Trickbot modular malware. Ursnif (aka Gozi) Banking Trojan malware. Sorted IPs for placing them in the blacklist. [09.12.2022]
- Malicious IP distributing attacks. November 28 – December 5, 2022.[09.12.2022]
- Weekly update 2022-12-02.pdf. Information about attacks that occurred in early December in European countries, from the Ragnar Locker Ransomware group. [05.12.2022]
- TLP_AMBER Ursnif IOCs November 21-27.zip [05.12.2022]
- NAECCS shares indicators related to network infrastructure Trickbot which is a modular malware that is used to steal information and drop ransomware. [24.11.2022]

- IPs causing the ransomware infection. Tables with each one attached. Guidance including techniques and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware attacks. [18.11.2022]
- Lithuanian defense center's weekly update on ransomware attacks that occurred in the first and second week of November in Ukraine and Bulgaria. Recommendations listed with the aim of preventing such attacks and other malicious activities. (Weekly update 2022-11-18.pdf)
  [18.11.2022]
- Chinese hackers target government agencies and defense bodies.pdf
  [16.11.2022]
- Ransomware (Ragnar Locker) affecting aviation pallets.pdf
  [08.11.2022]
- Weekly update 2022-10-28.pdf. DDoS and ransomware occurred last week in Ukraine and Poland (mainly in the financial sector) and Israel (Knesset Website).
  [31.10.2022]
- The FBI, CISA, HHS have released several Cyber Security Advisory and Guidance Information on Team Daixin, a cybercrime group that actively targets (throwing ransomware and data theft operations) US businesses, the healthcare sector and public health.
  [26.10.2022]
- Update of the Lithuanian Cyber Defense Center on Ransomware and DdoS attacks. Weekly update 2022-10-21.pdf [26.10.2022]

3. Finance and support services sector

For the National Authority on Electronic Certification and Cybersecurity, the budget allocated for 2022 is 57,952 thousand ALL, of which 53,952 thousand ALL Current Expenditures and 4,000 thousand ALL Capital Expenditures with internal financing.
In the following, we present in more detail the realization of expenses according to the allocated funds:

Calculation	Total	Fullfilled	%
600	30,122,400	24,382,994	81%
601	4,590,525	4,011,919	87%
602	18,876,000	5,728,198	30%
606	364,000	273,458	75%
231	4,000,000	702,000	18%
Amount	57,952,925	35,098,569	

Wages and Social Insurance Fund (items 600+601) The amounts allocated for wages and social insurance for 2022 are respectively 30,122,400 ALL for item 600 and 4,590,525 ALL for item 601. And the realization is respectively 24,382,994 ALL for item 600 and 4,011,919 ALL for article 601.

Fund for expenditure on goods and services (item 602) The amount allocated for the year 2022 for operational expenditure is ALL 18,876,000. And the realization for this item is 5,728,198 ALL.

Special Fund (item 606) The amount allocated for 2022 for expenses for disaster relief is 364,000 ALL. And the realization for this article is 273,548 ALL.

The Fund for Internal Investments (items 230+231), has been approved in the amount of 4,000,000 ALL in item 231. And the realization for this item is 702,000 ALL.

In October 2022, the employment relationships of the Authority's employees changed from civil servants to relationships according to the Labor Code.

During 2022, new recruitments were made, increasing the number of staff by 4 persons.