



WEEKLY BULLETIN

1-5 APRIL 2024

Quote

"Cybercrime is the biggest threat to every company in the world."

Ginni Rommety

of the week

Content:

- **Cyber Crisis Management Simulation Table**
- **The next awareness meeting within the campaign: "A safer cyberspace for children"**



Cyber Crisis Management Simulation Table

Deputy Prime Minister, Mrs. Belinda Balluku closely followed the simulation of the response to a cyber crisis, organized by NAECCS, in order to deepen cooperation and coordination between public and private institutions in such cases.

Organized in the House of Europe, this table, facilitated by eGA and NUKIB, within the project financed by the European Union for increasing capacities in the Western Balkans, brought together representatives at the decision-making level of institutions such as: National Agency of Information Society (AKSHI), the Ministry of the Interior, the Ministry of Infrastructure and Energy, the Ministry of Justice, the Ministry for Europe and Foreign Affairs, the General Prosecutor's Office, the State Information Service and representatives from the banking sector.

This table serves the effort to prepare a legal framework as complete as possible as well as the establishment of a team of experts who will be able to respond to malicious cyber-attacks in the country.



The next awareness meeting within the campaign: "A safer cyberspace for children"

On April 3, 2024, the next Workshop was organized in the premises of Cërrik Municipality, by NAECCS in cooperation with ASHMDF, within the awareness campaign "A safer cyber space for children".

This Workshop was developed within the framework of raising awareness among children and young people, that in addition to the positive benefits of using technology, attention should also be paid to the many risks they may face in cases of inappropriate use of the digital space.

Children, parents and all participants were informed that for any concern encountered while using social networks or different platforms where children's integrity is violated or they face psychological violence, abuse, display of inappropriate images, etc., they can report on the official website of NAECCS, on the REPORT button. They can also contact the Children's Helpline, Alo 116 111.

This meeting was attended by representatives of the local government, law enforcement institutions, social workers, children of different age groups from 9-year and secondary schools, teachers, parents, as well as representatives of local non-governmental organizations that play a role of important in protecting children.





WEEKLY BULLETIN

1-5 APRIL 2024

Quote

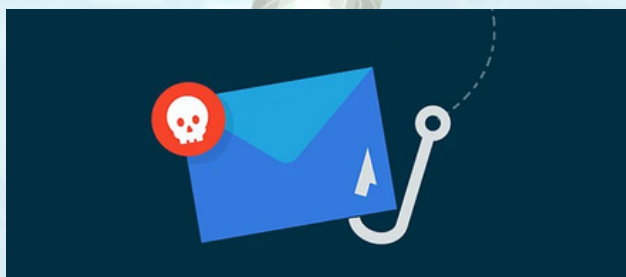
"Cybercrime is the biggest threat to every company in the world."

Ginni Rommety

of the week

Content:

- A new phishing campaign targeting oil and gas companies
- A new malware called Latrodectus is discovered
- City of Hope - Data Breach
- Microsoft Outlook - Patching Alert



A new phishing campaign targeting oil and gas companies

An updated version of information-stealing malware called *Rhadamanthys* is being used in phishing campaigns targeting the oil and gas sector.

The malware uses a unique vehicle incident lure and tricks the Federal Bureau of Transportation into a PDF with a hefty fine. The malware connects to a command and control (C2) server to collect sensitive data. The malware is provided by Cassandra Protector and delivered via an open source email tool called RoundCube.

[Link: Read more](#)



City of Hope - Data Breach

City of Hope, a cancer treatment and research center, has reported a data breach that exposed the sensitive information of over 820,000 patients.

Affected data includes full names, email addresses, phone numbers, dates of birth, social security numbers, driver's licenses, government IDs, bank accounts, credit card details, health insurance information and medical records. The center has implemented additional safeguards to prevent similar incidents. The type of cyber attack responsible for the breach remains unknown.

[Link: Read more](#)



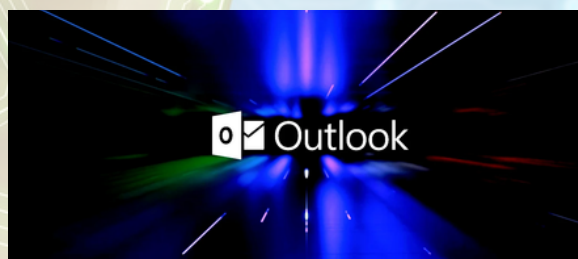
A new malware called Latrodectus is discovered

Researchers have discovered a new malware called Latrodectus, which is believed to be an evolution of the IcedID loader used in malicious email campaigns.

IcedID, first identified in 2017, was originally designed to steal financial information from infected computers. Over time, it became more sophisticated, adding evasion and command execution capabilities. Latrodectus is a downloader capable of returning other malicious payloads based on instructions received from a C2 - Command and Control server.

[Link: Read more](#)

PATCHING ALERT



Microsoft Outlook - Patching Alert

Microsoft has fixed an issue that causes incorrect Outlook security alerts when calendar.ICS files are opened after the December 2023 Outlook Desktop security updates.

The security updates fix the Microsoft Outlook information disclosure vulnerability CVE-2023-35636, which attackers could exploit to steal NTLM hashes via malicious files.

[Link: Read more](#)

