Countering ransomware. Summary of the international session „Together – safer, stronger, smarter"

The fifth edition of the international session "Together - safer, stronger, smarter" dedicated to the most pressing cybersecurity issues – took place on April 18th. This year, all participants have discussed challenges and various perspectives of countering ransomware - one of the biggest global cybersecurity challenge.

Ransomware is a type of malicious software, or malware that prevents the victim from accessing computer files, systems, or networks and demands to pay a ransom for the return of data. Especially in view of the fact that everyone can become potential target - from individuals to large, global organizations. It can happen anywhere and to anyone.

The topic and its' challenges was presented from different perspectives by the keynote speakers from the US Federal Bureau of Investigation, Government Information Security Office from the Republic of Slovenia, national CSIRTs from Poland (CSIRT NASK, CSIRT MoD), the U.S. Department of Homeland Security and Chancellery of the Prime Minister in Poland.

As stated by David Hitchcock, FBI Cyber Attaché, on one hand, the numbers of ransomware attacks, compared to previous year, have increased and continues to grow, as well as their complexity and general impact. Malware distributors have gotten savvy and technically advanced. On the other hand, the organizations are getting better at protecting and restoring data after an attack.

Still, the best way to protect and restore data are backups. There is still a need to raise awareness campaigns, community outreach, build trust between the victims and law enforcement and combine efforts to share information and engage both private-public sectors.

The ransom payment is still increasing and some organizations have serious dilemma as what to do: choose to pay ransom or

suffer major commercial and operational impact.

In most cases, the human factor is still the weakest point and as the quote says: we are as strong as our weakest link, therefore it should be underlined and repeated over and over again to stay cautious and use common sense. Beware of the risk and danger of downloading ransomware onto a computer by opening email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware.

Based on the survey conducted by Sophos[1] one of the problems is efficient use of available resources:

- invest in the right technology solutions
- have the skills and procedures in place:
- make backups and check them on regular basis to avoid potential disruption and loss of data;
- conduct security control ensuring high quality defenses;
- proactively search for potential threats and vulnerability, closing down the security gaps;
- prepare the procedures in case of an attack: what to do and who to contact.

One of the proactive solutions is to purchase insurance coverage against cyberattacks.

Another challenge associated with ransomware, raised by Uroš Svete, Director for Government Information Security Office from the Republic of Slovenia is classification of ransomware based on the target, perpetrators, different types of attack. Was it encrypted or leaked? Was it economic espionage or extortions? Who is responsible for allowing it to happen. Is it end user's fault, the IT manager or the CEO of the company?

New raising challenge directly connected to ransomware is implementation of artificial intelligence which can also be used by the perpetrators.

Maciej Siciarek, Director of CSIRT NASK has focused on the technical support and incident response who stated that the role of CERT has grown and added a duty to assist companies to recover data, provide forensic support, provide instructions and ransomware guidelines.

Representative from the Command of Cyberspace Defense Forces, CSIRT MoD has presented a case study on one of the ransomware attacks conducted in Poland.

Reliable and responsible following through the procedures before the incident is one of the key factors to prevent and minimize the loss.

[1] https://www.sophos.com/en-us/content/state-of-ransomware

Ian Hansen, Deputy Director for International Cyber Policy at the U.S. Department of Homeland Security (DHS), confirmed that the extent of the threat is broad. He further mentioned how the Colonial Pipeline ransomware attack was a turning point showing how interconnected the cybersecurity environment is and the effect and impact attacks can have on critical infrastructure facilities. Hansen added that nearly 85% of U.S. critical infrastructure is owned by the private sector, therefore good communication and information sharing is a must and more important than ever. Due to evolving methods and the need to increase resilience, DHS has adopted a comprehensive approach and combined capabilities and resources with other U.S. federal agencies, law enforcement, private sector and foreign partners to share information and mitigate threats. DHS has also offered a wide variety of resources from educational websites, engagement on cybersecurity hygiene, tools such as the Ransomware Vulnerability Warning Pilot which scans systems for malware and suggests mitigation techniques and guidance on other proactive steps and activities that organizations of all sizes can take. DHS' Cybersecurity and Infrastructure Agency (CISA) is front and center of many of these efforts, and also joins other federal agencies releasing cyber alerts, security exploits, advisories. CISA also leads the Joint Cyber Defense Collaborative with the acknowledgement that a collective approach with the private sector is the only way to efficiently combat ransomware and other threats.

Acknowledging the problem, in 2021 the White House has invited a number of countries to create and join Counter Ransomware Initiative. So far, CRI gathered over 40 countries around the world committed to build collective resilience to ransomware, cooperate to disrupt ransomware and pursue the actors/hackers who are responsible, countering illicit finance that underpins the ransomware ecosystem.

Building the effective resilience to ransomware attacks requires effective policies and cooperation with trusted partners therefore the CRI has created a voluntary International Counter Ransomware Initiative Task Force to develop cross-sectoral tools and cyber threat intelligence exchange to increase early warning capabilities and prevent attacks, as well as consolidate policy and best practice frameworks.

Poland is part of the CRI and newly created CRI Task Force (CRITF). Marcin Domagała from the Chancellery of the Prime Minister Office has presented Polish initiative to support and develop CRITF.

The CRI is committed not only to protect ourselves and each other from ransomware, but also to help other countries protect and disrupt so that ransomware is unable to gain traction worldwide. To that end, the goal is to share technical and threat information and provide protection and recommendations as broadly as possible.

As we all know there are challenges at each step of the way. I am hoping that this meeting has enriched our knowledge and pointed out to different solutions, perspectives which is worth considering