Гіневська В., студент Національної академії внутрішніх справ
Language adviser:*Mogilevska V.*

DARKNET CYBERCRIME THREATS TO SOUTHEAST ASIA

Awareness is fundamental for addressing cybercrime. Given, however, the challenges posed by darknets, stakeholders must increase their commitment and cooperation to developing policy, sharing intelligence and enhancing international cooperation to counter darknet crime nationally, regionally and internationally.[1]

The use of darknets and the Darkweb has increased in recent years, and the COVID-19 pandemic also appears to have further exacerbated the trend, including by criminals with no prior cyber experience. Darkweb forums normally dedicated to narcotics have begun offering COVID-19-related merchandise including fraudulent COVID-19 vaccines, hydroxychloroquine, and personal protective equipment. New users have also started seeking support from more experienced darknet criminals about criminal opportunities. [2]

Bangkok - The United Nations Office on Drugs and Crime (UNODC) delivered a practical regional training on ransomware investigations to law enforcement officers, computer security incident response teams, and prosecutors from Malaysia, the Philippines and Thailand.

The increased digitalization of society, compounded by the COVID-19 outbreak, has contributed to a recent 600% rise in cybercrimes in Southeast Asia. Within this rise, ransomware has skyrocketed to become the most prominent malware threat.

Ransomware is a malicious software that, once gaining access and being installed on your device, will encrypt all the data and require a ransom to be paid to return access to the data. Unfortunately, paying the ransom does not in any way guarantee access will be granted to the data. Experts estimate that ransomware attacks will globally occur every 11 seconds, resulting in total damage costs of US$ 20 billion in 2021.

These trends are being driven by an increase in the number of available targets, as well as the perception of cybercrime as highly profitable with a relatively low risk of detection. The criminals target not only the individuals, but increasingly focus on critical national infrastructure and business of all sizes in both the private and public sectors.

The significant threat of ransomware, known to disrupt essential services such as (public) healthcare, schools/colleges, finance, insurance, government functions and critical infrastructure, has become a serious

global concern and a matter of national security for numerous countries around the world.

In September 2021, a Malaysian web-hosting service was the target of a ransomware attack demanding US$ 900,000 in cryptocurrency. In May 2021, four subsidiaries of an international insurance company in Thailand, Malaysia, Hong Kong and the Philippines were hit by a ransomware attack asking for US$ 20 million. Similar attacks also took place last September in Thailand, where computer systems and data of several hospitals, companies and organizations were encrypted and blocked.

"Ransomware attacks have skyrocketed in the past years, increasingly targeting critical national infrastructures, disrupting business processes, and compromising vital data that they require to function. There needs to be a collaborative and coherent response to these threats, and UNODC has been working closely with Member States to strengthen their national and cross-border operational capacity to respond to ransomware", said Mr. Alexandru Caciuloiu, UNODC Cybercrime and Cryptocurrency Advisor for Southeast Asia and the Pacific.[3]

The INTERPOL's ASEAN Cybercrime Operations Desk (ASEAN Desk) with the support from law enforcement agencies in the region and INTERPOL's private sector cybersecurity partners identify the region's top cyberthreats:

- Business E-mail Compromise campaigns continue to top the chart with businesses suffering major losses, as it is a high-return investment with low cost and risk.
- Phishing. Cybercriminals are exploiting the widespread use of global communications on information related to COVID-19 to deceive unsuspecting victims.
- Ransomware. Cybercrime targeting hospitals, medical centers and public institutions for ransomware attacks has increased rapidly as cybercriminals believe they have a higher chance of success given the medical crisis in many countries.
- E-commerce data interception poses an emerging and imminent threat to online shoppers, undermining trust in online payment systems.
- Crimeware-as-a-Service puts cybercriminal tools and services in the hands of a wider range of threat actors – even non-technical ones, to the extent that anyone can become a cybercriminal with minimal 'investment'.
- Cyber Scams. With the increase of online transactions and more people working from home, cybercriminals have revised their online scams and phishing schemes, even impersonating government and health authorities to lure victims into providing their personal information and downloading malicious content.

• Cryptojacking continues to be on the radar of cybercriminals as the value of cryptocurrencies increases.

"Cybercrime is constantly evolving. The COVID-19 pandemic has accelerated digital transformation, which has opened new opportunities for cybercriminals," said Craig Jones, INTERPOL's Director of Cybercrime.

"Through this report, INTERPOL strives to support member countries in the ASEAN region to take a targeted response against ever-evolving cybercrime threats to protect their digital economies and communities," added Mr Jones.[4]

Darknet criminal marketplaces have become more popular during the COVID-19 pandemic, due to a combination of technologies offering greater anonymization for both sellers and buyers. Features such as escrow payment systems and reputation metrics have increased. Cryptocurrencies are the payment method of choice, and while law enforcement try to identify the criminal end-users, the use of crypto-mixers, tumblers, or laundry services break the link between the initial purchase of cryptocurrencies and the final payment destination. This makes it more difficult for law enforcement to follow the money and bring high-risk offenders to justice. Alexandru Caciuloiu, Cybercrime and Cryptocurrency Advisor, highlighted that Bitcoin remains the main cryptocurrency used on the Darknet, but privacy coins such as Monero, Litecoin and Bitcoin Cash are perceived as offering greater anonymity to cybercriminals.

Список використаних джерел

1. https://nysean.org/blog/2021/2/25/darknet-cybercrime-threats-to-southeast-asia-2020
2. https://ct-morse.eu/resource/darknet-cybercrime-threats-to-southeast-asia/
3. https://thailand.un.org/en/152525-ransomware-attacks-growing-threat-needs-be-countered
4. https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia