УДК 004.491
Marharyta Stichuk[1], Nataliia Zhukova[2]
[1]student of group CST-220, National University «Zaporizhzhia Polytechnic»
[2]PhD (Philology), assistant prof. National University «Zaporizhzhia Polytechnic»

DEVELOPMENT TRENDS IN CYBERSECURITY

The year 2020 was without a doubt one of the most consequential and transformational in recent memory: a global pandemic, economic shocks impacting millions of people's lives, and social and political unrest.

As per the World Economic Forum's Global Risks Report 2021, cyber risks continue ranking among global risks. The COVID-19 pandemic has accelerated technological adoption, yet exposed cyber vulnerabilities and unpreparedness. Cybercrime's attack surface has increased because of the switch to home working.

Common types of cyber-attacks are as follows:

1. malware (malicious software, including spyware, ransomware, viruses, and worms);

2. phishing (fraudulent communications that appear to come from a reputable source, usually through email);

3. man-in-the-middle attack (MitM, occurs when attackers insert themselves into a two-party transaction);

4. denial-of-service attack (DDoS, floods systems, servers, or networks with traffic to exhaust resources; as a result, the system is unable to fulfill requests);

5. a Structured Query Language (SQL) injection (occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not);

6. a zero-day exploit (hits after a network vulnerability has announced but before a patch or solution has implemented; attackers target the disclosed vulnerability during this window of time);

DNS Tunneling (utilizes the DNS protocol to communicate non-DNS traffic over port 53). They can be used to masking outgoing traffic as DNS, concealing data that has typically shared through an internet connection. For malicious use, DNS requests are used to filter data from a hacked system to the attacker's infrastructure. It can also be used for command and control callbacks from the attacker's infrastructure to a hacked system.

So far this year, we have seen some big-name companies, with supposedly first-class security, become victims: World Health Organization, Twitter, Zoom, Magellan Health, Marriott International, MGM Resorts, SolarWinds.

IBM Security X-Force drew on billions of data points collected from their customers and public sources between January and December 2020 to analyze attack types, infection vectors, and global and industry comparisons. The following are some of the top findings presented in the X-Force Threat Intelligence Index:

1. 23% Ransomware share of attacks. $123 million+ estimated profits from top ransomware.

2. 35% Scan-and-exploit share of top infection vectors. #2 Manufacturing rank in top attacked industries.

3. 49% ICS-related vulnerability growth rate, 2019-2020.

Top 3 attack types are:

1. Ransomware (23% of attacks)
2. Data theft (160% increase since 2019)
3. Server access (233% increase since 2019)

Top 3 initial attack vectors include

1. Scan-and-exploit (35% of attacks vs. 30% in 2019)
2. Phishing (33% of attacks vs. 31% in 2019)
3. Credential theft (18% of attacks vs. 29% in 2019)

Security Trends for 2021 are the following:

1. Rise of Automotive Hacking
2. Integrating AI with Cyber Security
3. Mobile is the New Target
4. Cloud is Also Potentially Vulnerable
5. Data Breaches: Prime target
6. IoT with 5G Network: The New Era of Technology and Risks