1. Статистика кібератак у 2020 році

2020 року фахівці Cyber Polygon з безпеки нарахували понад **900 кіберзлочинців** і понад **1 млрд шкідливих програм.**

Загрози класифіковані за трьома рівнями:

Нижній рівень (94%) — найпримітивніші атаки.

- фішингові сайти на тему COVID-19: допомога в отриманні допомог та компенсацій, підроблені сертифікати про вакцинації та QR-коди;
- шахрайства з доставкою товарів і послуг;
- дзвінки шахраїв, які представляються службою безпеки банку і виманюють дані карток.

Середній рівень (5%) — це атаки програм-вимагачів, кожна четверта з яких припала на корпоративних користувачів. Яскраві приклади:

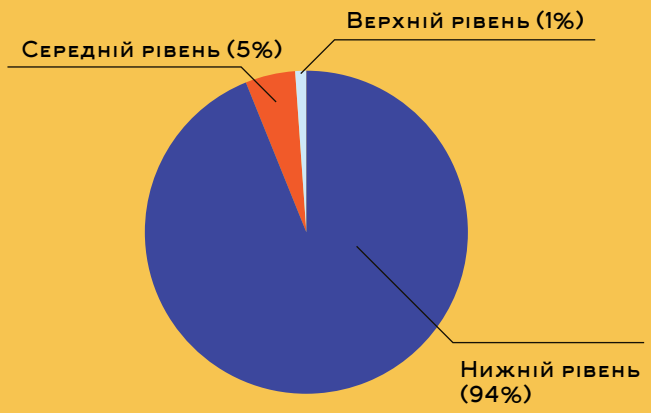
- атака на мережу американських заправок Colonial Pipeline: привела до їх повного колапсу;
- атака на ірландську службу охорони здоров'я: в результаті люди не могли записатися на вакцинацію або на прийом до лікаря.

Верхній рівень (близько 1%) — найскладніші та точно спрямовані атаки, на розслідування яких іноді витрачаються роки.

> 900 кіберзлочинців

> 1 млрд шкідливих програм

Класифікація загроз за рівнями



Будьте уважні до будь-яких листів, яких не очікували.

2. Грудень 2018: кібератака проти німецьких політиків

Хакери оприлюднили **особисті дані** сотень німецьких політиків, журналістів і знаменитостей. Цю атаку назвали одним із найбільших **порушень кібербезпеки** країни.

Витік інформації містив:

- мобільні **номери** та **адреси** депутатів;
- електронні **листи**;
- **дані** інтернет-переписки та кредитних карток;
- копії **документів**, що посвідчують особу, та договори оренди;
- голосові **повідомлення** від партнерів та дітей.

Дані було зламано з приватних облікових записів електронної пошти, а також їхніх записів у соціальних медіа, як-от Facebook та Twitter.

Принаймні два депутати помітили збої в роботі своїх облікових записів за декілька місяців до атаки.

Помітили підозрілу діяльність? Повідомте IT-спеціалісту вашої організації або CERT-UA.