Organization for Security and Co-operation in Europe
Project Co-ordinator in Ukraine

Кібербезпека та Кібергігієни: Основні тенденції

osce.org

• Демид Майорников • Version x (xx.xx.08)

Зміст

Актуальність кібербезпеки та кібергігієни

Розуміння портрету зловмисників

- Типи хакерів
- Мотивація

Ланки кібербезпеки

Принципи кібербезпеки

Типи загроз

Вразливості

Актуальність тематики кібербезпеки

Існує великий хайп навколо тематики кібербезпеки та кібергігієни.

А чи дійсно це актуально?

- CheckPoint
- Fortinet

Приклад
Кібератака на трубопровід: Colonial Pipeline



Актуальність тематики кібербезпеки

Статистики.

- 2021 року світові збитки від кіберзлочинності сягатимуть $6 трильйонів доларів щорічно. (Cybersecurity Ventures)
- У першій половині 2020 року до зливів потрапили 36 мільярдів записів. (RiskBased)
- 45% всіх витоків даних включали хакінг, 17% шкідливе ПЗ та 22% фішинг. (Verizon)

Розуміння портрету зловмисників

BLACK HAT



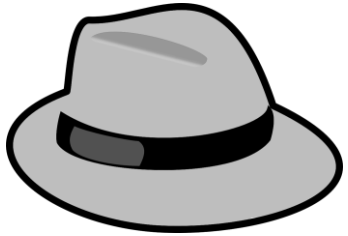
- **Вчиняють кіберзлочини**
- **Порушують комп'ютерну безпеку із зловмисною метою або для особистої вигоди**

WHITE HAT



- **Етичні хакери**
- **Захищають системи**

GREY HAT



- **можуть порушувати закони або типові етичні норми, але не мають зловмисного наміру притаманного для хакера**

Розуміння портрету зловмисників

Кіберзлочинці мають різні мотивації у скоєнні злочинів.

Які мотивації існують?

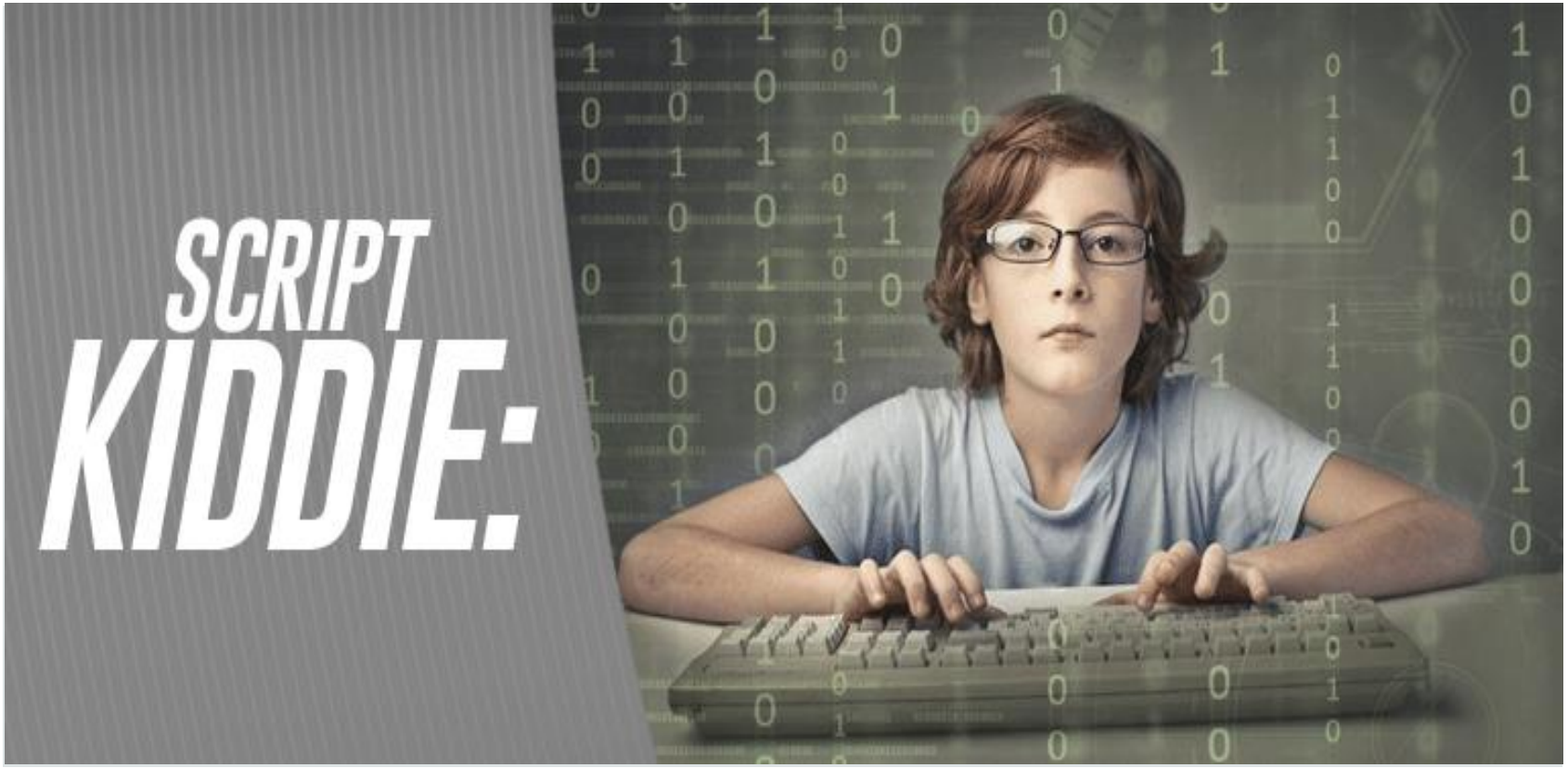
Фінансова мотивація



Ідеологічна мотивація

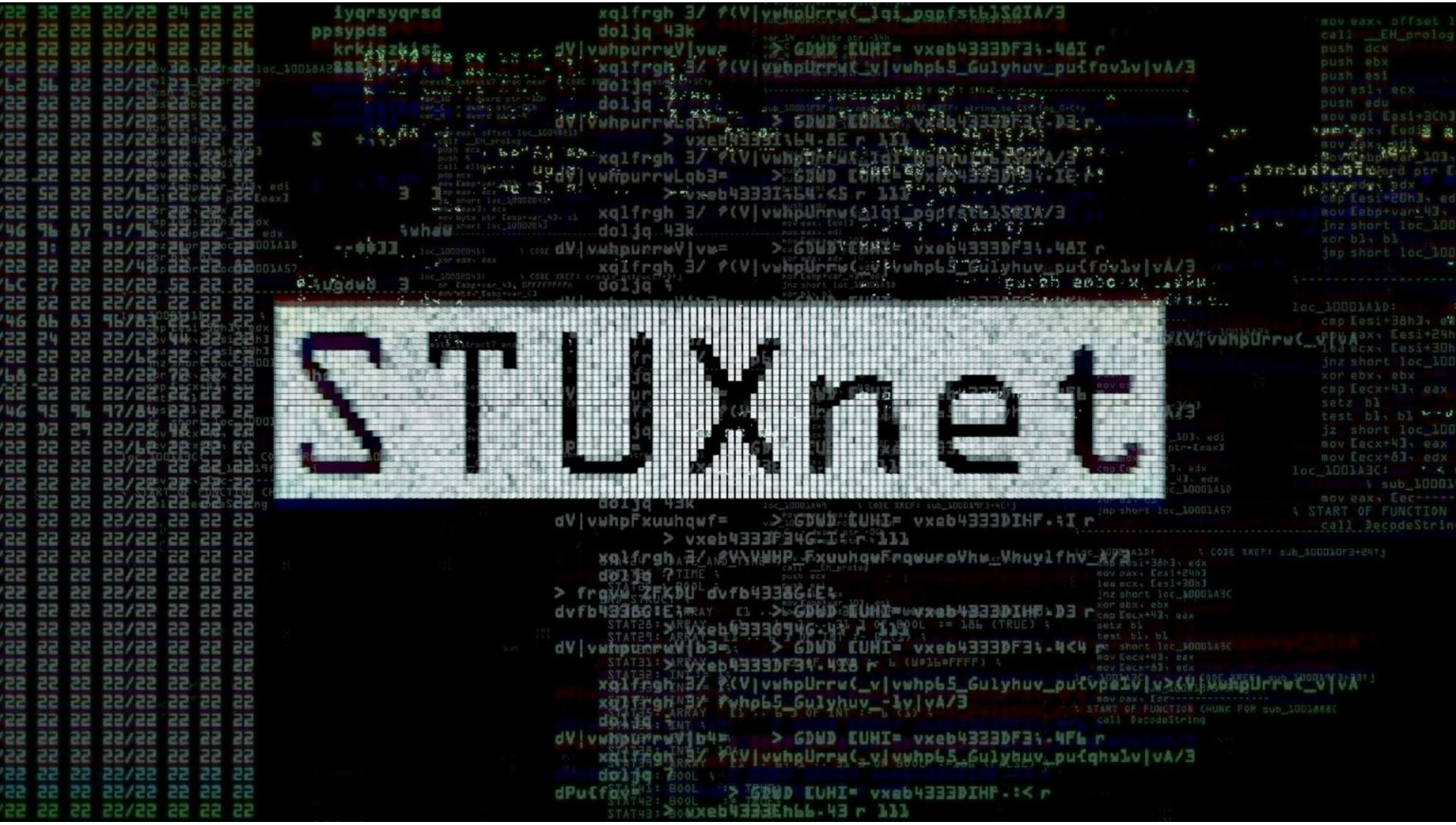


Мотивація “Розвага”



Політична мотивація





Organization for Security and
Co-operation in Europe
Project Co-ordinator in Ukraine

Ланки кібербезпеки

Безпека складається з **3 основних ланок:**

- Люди
  - Усвідомлення членами організації кібер загроз та протидія їм.
- Процеси
  - Побудова процесів, які контролюють безпеку організації: розподіл відповідальностей, управління ризиками, інвентаризація, та інше.
- Технології
  - Розробка та налаштування систем, які відповідають принципам інженерії безпеки (приклад: принцип мінімальних привілеїв)

Цікавий факт:

“95% всіх порушень безпеки спричинені через **помилку людини”**

Cybint

Принципи кібербезпеки

У кібербезпеці виокремлюють **3 основні принципи:**

- **Конфіденційність**
  - Тільки авторизовані особи мають мати доступ до інформації
- **Цілісність**
  - Тільки авторизовані особи можуть змінювати зміст інформації
- **Доступність**
  - Авторизовані особи мають завжди мати доступ до інформації

Які принципи кібербезпеки порушують наступні загрози?

- Атака на відмову в обслуговуванні - DoS/DDoS
- Людина посередині - man-in-the-middle
- ПЗ Вимагач - ransomware
- Зчитувач клавіатури - кілогер
- Бекдор - віддалений доступ

Типи вразливостей

Вразливості поділяють на **2 категорії:**

- **Відомі вразливості**
  - Існує публічна база всіх відомих вразливостей
- **Вразливості нульового дня**
  - Вразливості, про які не знає компанія розробник

Публічна база вразливостей

CVE Details
The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) Search / View CVE

og In Register

Vulnerability Feeds & Widgets[New] www.itsecdb.com

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact

Microsoft : Security Vulnerabilities Published In 2019 (Denial Of Service)

2019 : January February March April May June July August September October November December CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-1347	119		DoS Overflow	2019-10-10	2019-10-15	7.1	None	Remote	Medium	Not required	None	None	Complete
A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1343, CVE-2019-1346.														
2	CVE-2019-1346	119		DoS Overflow	2019-10-10	2019-10-15	7.1	None	Remote	Medium	Not required	None	None	Complete
A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1343, CVE-2019-1347.														
3	CVE-2019-1343	119		DoS Overflow	2019-10-10	2019-10-15	7.1	None	Remote	Medium	Not required	None	None	Complete
A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1346, CVE-2019-1347.														
4	CVE-2019-1326	20		DoS	2019-10-10	2019-10-11	7.8	None	Remote	Low	Not required	None	None	Complete
A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.														
5	CVE-2019-1317	59		DoS	2019-10-10	2019-10-11	5.6	None	Local	Low	Not required	None	Partial	Complete
A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'.														
6	CVE-2019-1301	20		DoS	2019-09-11	2019-09-12	5.0	None	Remote	Low	Not required	None	None	Partial
A denial of service vulnerability exists when .NET Core improperly handles web requests, aka '.NET Core Denial of Service Vulnerability'.														
7	CVE-2019-1292	119		DoS Overflow	2019-09-11	2019-09-12	6.8	None	Remote	Low	Single system	None	None	Complete
A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'.														