МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Управління кіберінцидентами та аналіз подій»

**Канал електронної комунікації як вектор нав’язування payload**

Дата 20.04.2024

**Виконав:** курсант навчальної групи 314

старший солдат \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Семенюк О.О.

**Перевiрив:** викладач кафедри № 33

капітан\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Прийма О.О.

Київ – 2024

Військовою частиною надано файл дампу “AgentTesla\_ZSU\_case.pcap”, який слід завантажити в Wireshark.

Отже, мені було надано PCAP-файл з ймовірною шкідливою активністю, та провівши аналіз я визначив :

1. IP-адреса жертви : 192.168.100.14.

2. IP-адреса зловмисника : 107.161.178.166.

3. Протокол (канал) що використано зловмисником для ексфільтрації данних жертви : FTP.

4. Ім’я хоста жертви : USER-PC.

5.Логін який використовувався зловмисником для аутентифікації на FTP сервері : amani@artrsllc.com.

6. Пароль який використовувався зловмисником для аутентифікації на FTP-сервері : WY{9+?ae}qt.

7. Дата і час початку передачі викраденої інформації від жертви [YYYYMM-DD HH:MM:ss] : 11.07.2022 17:30:03.77.

8. Назва файлу що був завантажений з ексфільтрованими даними : PW\_admin-USER-PC\_2022\_07\_11\_22\_30\_00.html.

9. Загальний об’єм інформації, що було викрадено у жертви : 567 bytes.

10. Назва і версія операційної системи, що встановлена у жертви : Microsoft Windows 7Professional.

11. Марка та модель процесора на ПК жертви : Intel CORE i5-6400.

12. Обліковий запис жертви для поштового клієнту : [honey@pot.com](mailto:honey@pot.com) , Outlook.

13. Браузери з яких були викрадені облікові записи жертви : FireFox , Chrome.