МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Управління кіберінцидентами та аналіз подій»

**ПРИНЦИПИ ОРГАНІЗАЦІЇ IP-ПІДМЕРЕЖ**

Варіант № 9

Дата 21.04.2024

**Виконав:** курсант навчальної групи 314

ст. солдат \_\_\_\_\_\_\_\_\_\_\_\_\_КОНДРАТЕНКО Є.А.

**Перевiрив:** викладач кафедри № 33

капітан\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ПРИЙМА О.О.

Київ – 2024

**Завадання:**

Дослідити ситуацію, як експерти з ІБ, яка відбулася з одним з офіцером деякої військової частини. Було викрадено інформацію після надходження листа з вкладенням, що містило файл-презентацію «Відновлено виплату 30 тисяч військовослужбовцям» з адреси minfin\_zsu@gmail.com. Військовою частиною надано файл дампу “AgentTesla\_ZSU\_case.pcap”, який слід завантажити в Wireshark.

Отже, Вам надано PCAP-файл з ймовірною шкідливою активністю, вашим завданням буде визначити:

1. IP-адреса жертви.

2. IP-адреса зловмисника.

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

4. Ім’я хоста жертви.

5. Логін який використовувався зловмисником для аутентифікації на FTPсервері.

6. Пароль який використовувався зловмисником для аутентифікації на FTP-сервері.

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

8. Назва файлу що був завантажений з ексфільтрованими даними.

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

10. Назва і версія операційної системи, що встановлена у жертви.

11. Марка та модель процесора на ПК жертви.

12. Обліковий запис жертви для поштового клієнту.

Браузери з яких були викрадені облікові записи жертви. Додаткові завдання\* (для бажаючих):

13. Альтернативні способи визначення хоста жертви?

14. Визначте геолокацію IP адреси зловмисника.

15. Підготуйте технічні рекомендації для внесення змін до політик безпеки з метою блокування даної активності в ІКС ЗС України, а також пропозиції фахівцям захисту інформації та кібербезпеки щодо недопущення у подальшому подібних інцидентів (на підставі п.2.13 Наказу Головнокомандувача Збройних Сил України від 23.10.2021 № 322 “Про затвердження Інструкції з організації реагування на інциденти кібербезпеки у Збройних Силах України”)

**Висновок:**

Проведений аналіз виявив різноманітні дані, що можуть бути вкрадені шляхом електронної пошти та зловмисних програм. Відстеження PCAP-файлу дозволило виявити важливі відомості, такі як IP-адреси злочинця та жертви, протокол, використаний для пересилання даних, а також інші параметри, такі як об'єм вкраденої інформації та технічні характеристики комп'ютера потерпілого.

**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 (File Transfer Protocol)

**4. Ім’я хоста жертви.**

USER-PC

**5. Логін який використовувався зловмисником для аутентифікації на FTPсервері.**

amanni@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].**

Arrival Time: Jul 12, 2022 00:30:03.777001000 Фінляндія (літо)

**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

**10. Назва і версія операційної системи, що встановлена у жертви.**

OSFullName: Microsoft Windows 7 Professional

**11. Марка та модель процесора на ПК жертви.**

CPU: Intel(R) Core(TM) i5-6400 CPU @ 2.70GH

**12. Обліковий запис жертви для поштового клієнту.**

Username:honey@pot.com  
 Password:honeypass356

**13. Браузери з яких були викрадені облікові записи жертви. Додаткові завдання\* (для бажаючих):**

Chrome; Firefox