שיעור 12

**תרגיל: 0rphan - הסוף**

המשטרה ממשיכה לחפש את ההאקר 0rphan, פושע ה-Ransomware המפורסם. כעת מתברר כי הוא ישראלי, עונה לשם אור פנדובסקי ועבד בעבר כאיש מכירות בחברת BUG, סניף רעננה. כדי למצוא איתו חברת BUG הסכימה לתת למשטרה גישה למערכת ניהול העובדים של החברה. על פי הדיווחים, המערכת שומרת את המיקומים המדויקים מהם התחבר 0rphan לשרת, אך אבוי - התוכנה של BUG לא עובדת ואף אחד לא יודע למה. עזרו למשטרה למצוא פרטים על מיקומו הנוכחי של 0rphan שיעזור להם למצוא אותו.

**שלב א'**

פתחו את תוכנת העובדים של BUG המצורפת בקובץ BugClient.zip ונסו לדלות ממנה מידע אודות הכניסות של 0rphan למערכת.

לצורך הפתרון עליכם להשתמש בכל הכלים אשר למדנו השנה –

Wireshark, Putty, קובץ hosts

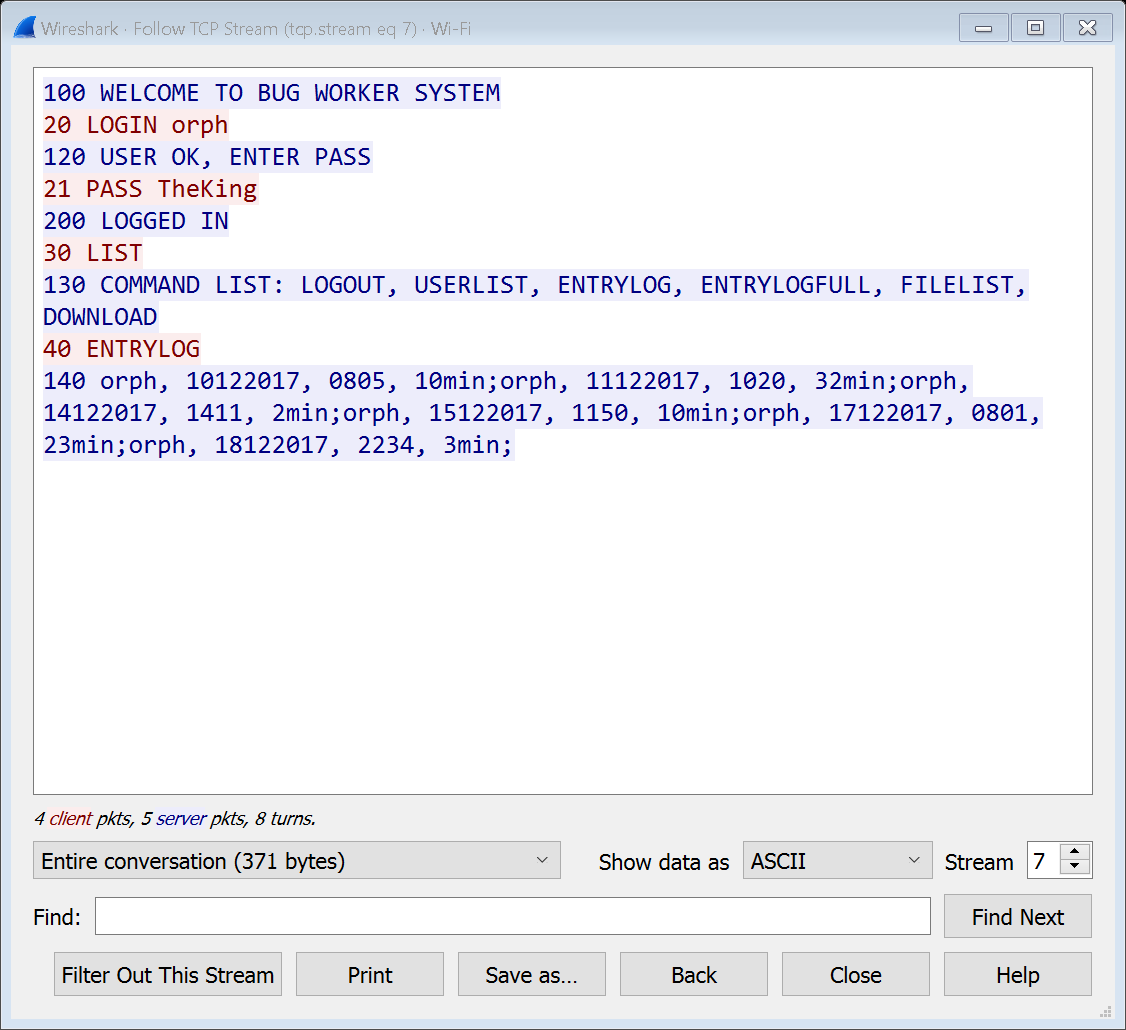
משימתכם היא למצוא את מסלול הבריחה של 0rphan (בתחנות).

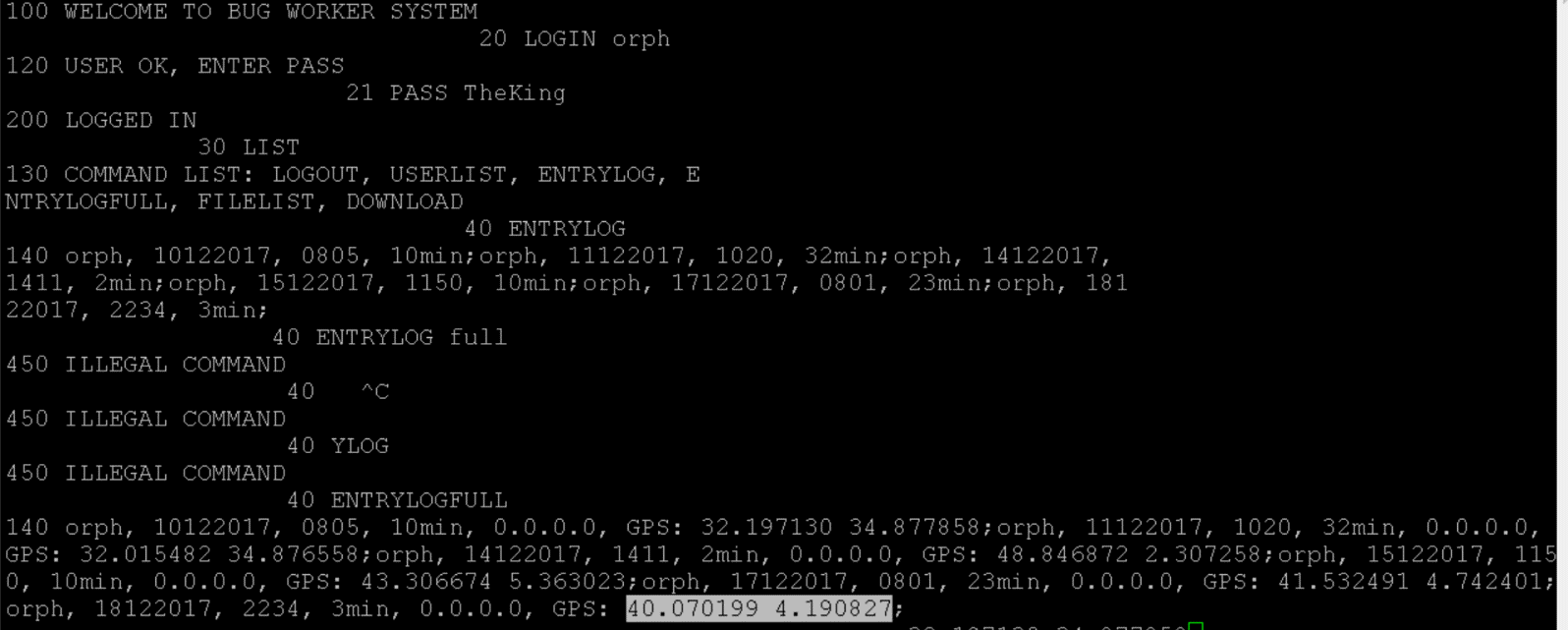
בהצלחה!

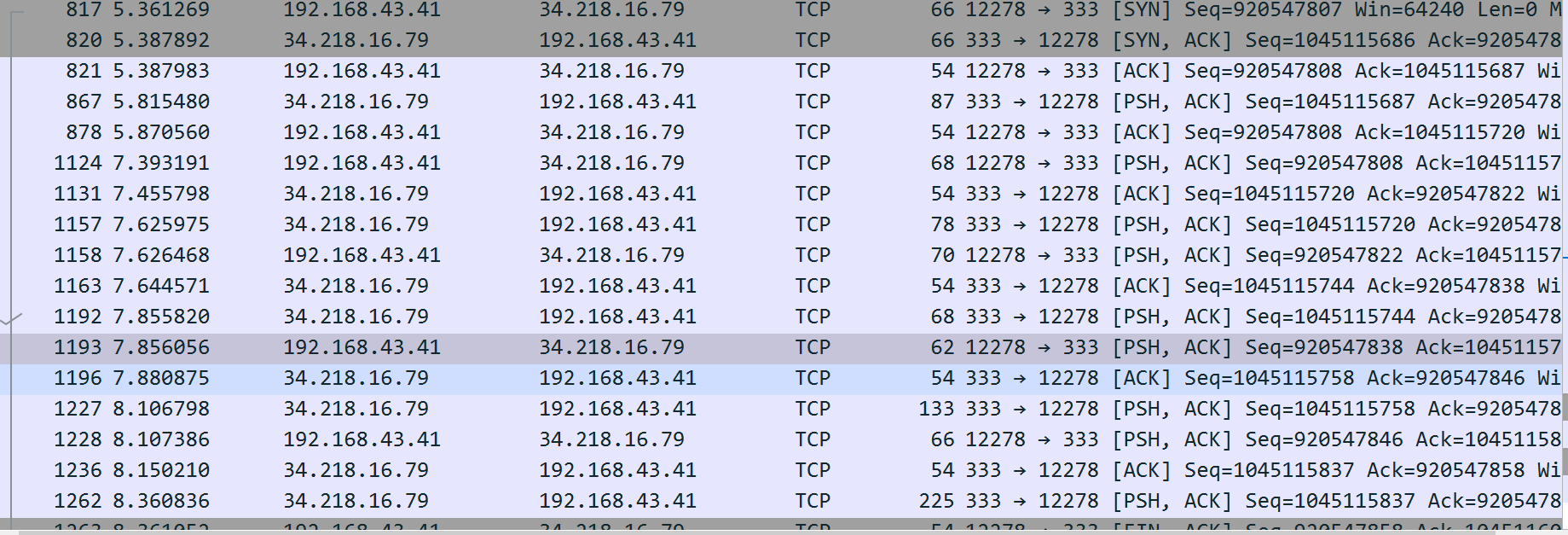
1. מהם המיקומים בהם שהה 0rphan? איפה הוא נמצא כיום לדעתכם?

|  |
| --- |
| קניון רננים 32.197130 34.877858  נמל תועפה בן גוריון 32.015482 34.876558  **156Bis Avenue de Suffren(פריז צרפת) 48.846872 2.307258**  **Les Terrasses du Port(צרפת) 43.306674 5.363023**  **41.532491 4.742401)אמצע הים)**  **Mar Mediterrània 40.070199 4.190827**  **Es Mercadal(אי כל שהוא שנחשב ספרד) (40.070199 4.190827**  18.12.2017 כול הנראה שהוא באי הספרדי |

1. ספרו מהו התהליך אותו עשיתם כדי להגיע לפתרון. נסו לפרט ככל האפשר. צרפו צילום מסך רלוונטי.





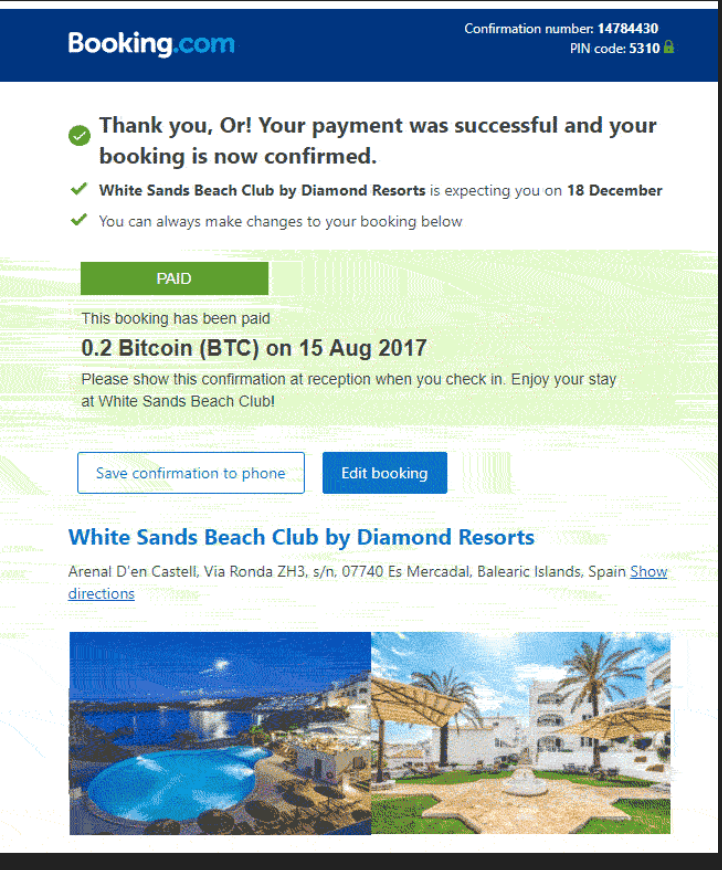


|  |
| --- |
| קודם כל הסנפתי כש ניסיתי ליהיכנס פעם הראשונה  גיליתי שם שהשרת שינה את הip שלו  אז שיניתי את זה בקובץ HOSTS  ניכנסתי דרך התוכנה  ראיתי בהספות את כל הפקודות  נכנסתי דרך הtelenet  ושם יש פקודה שמראה מתי נכנסו ובאיזה מיקום  אז חיפשתי לכל את המיקום |

**שלב ב'**

על פי הדיווחים, בחשבונו של 0rphan ב-BUG אוחסן קובץ שעשוי להיות משמעותי למציאתו. נסו להוריד אותו.

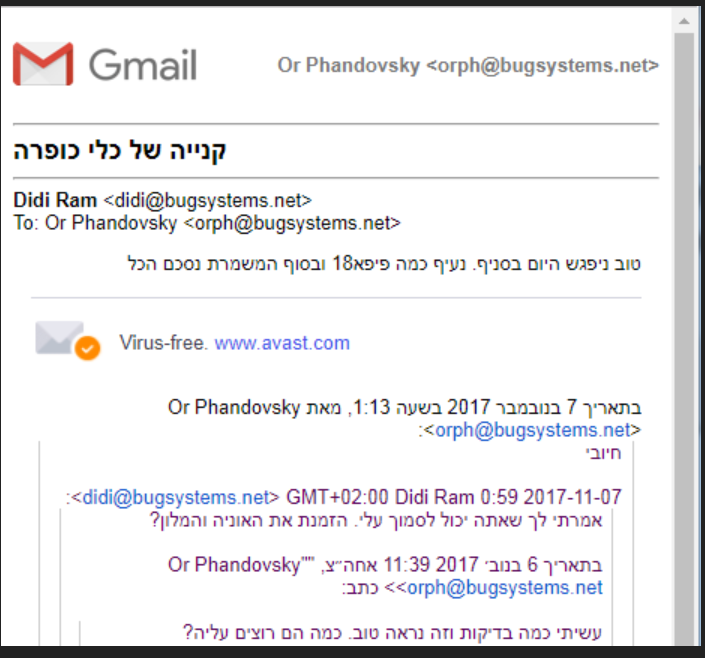
1. צרפו צילום של הקובץ והסבירו כיצד השגתם אותו.

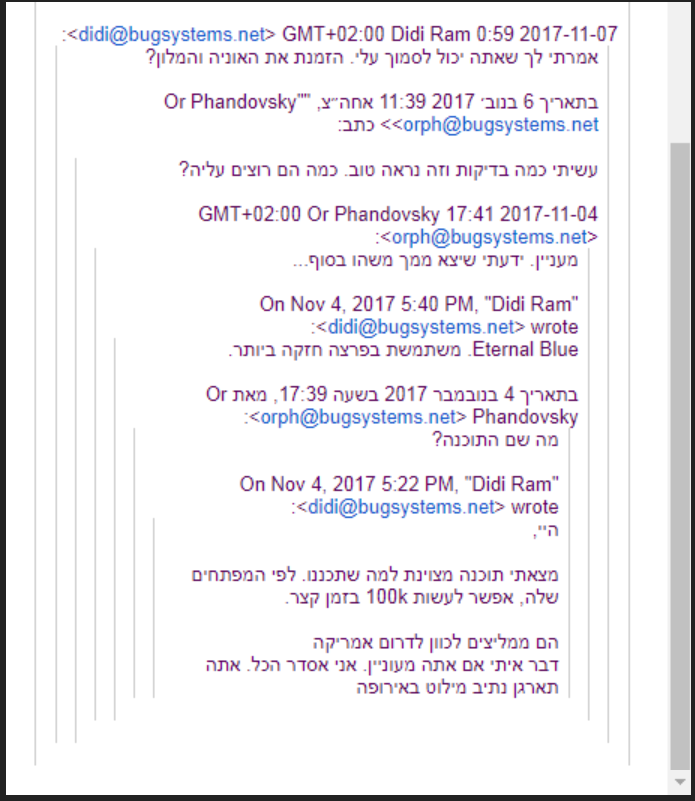


|  |
| --- |
| ב טלנט עשיתי את הפקודה 40 FILELIST כדי לראות איזה פיילים יש  ואז DOWNLOAD לפייל  ואז דיקוד לביס 64 פייל |

**בונוס - שלב ג'**

בחקירה התברר כי מנהל המשמרת בסניף BUG בו עבד 0rphan, דידי רם, שיתף איתו פעולה בתכנון הפשעים. נסו למצוא בפרוטוקול **חולשה** שתאפשר לכם להשיג מידע מפליל אודות.

1. הסבירו מהי החולשה בפרוטוקול וכיצד ניתן לנצל אותה. צרפו צילום של הקובץ שמצאתם.



|  |
| --- |
| מ סיבה כל שהיא אם כש אתה בתוך החשבון של אור ומנסה לעשות לוגין לחשבון של דידי זה לא מבקש סיסמה |
|  |