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).

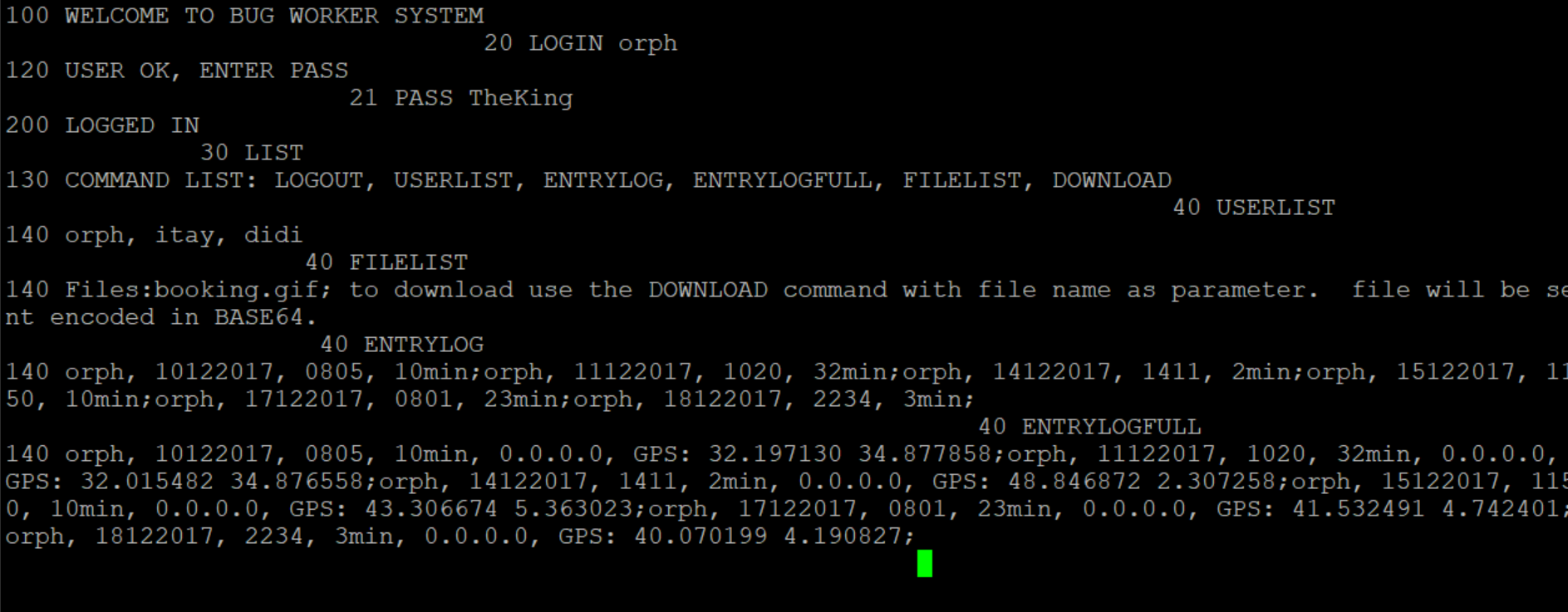
בהצלחה!

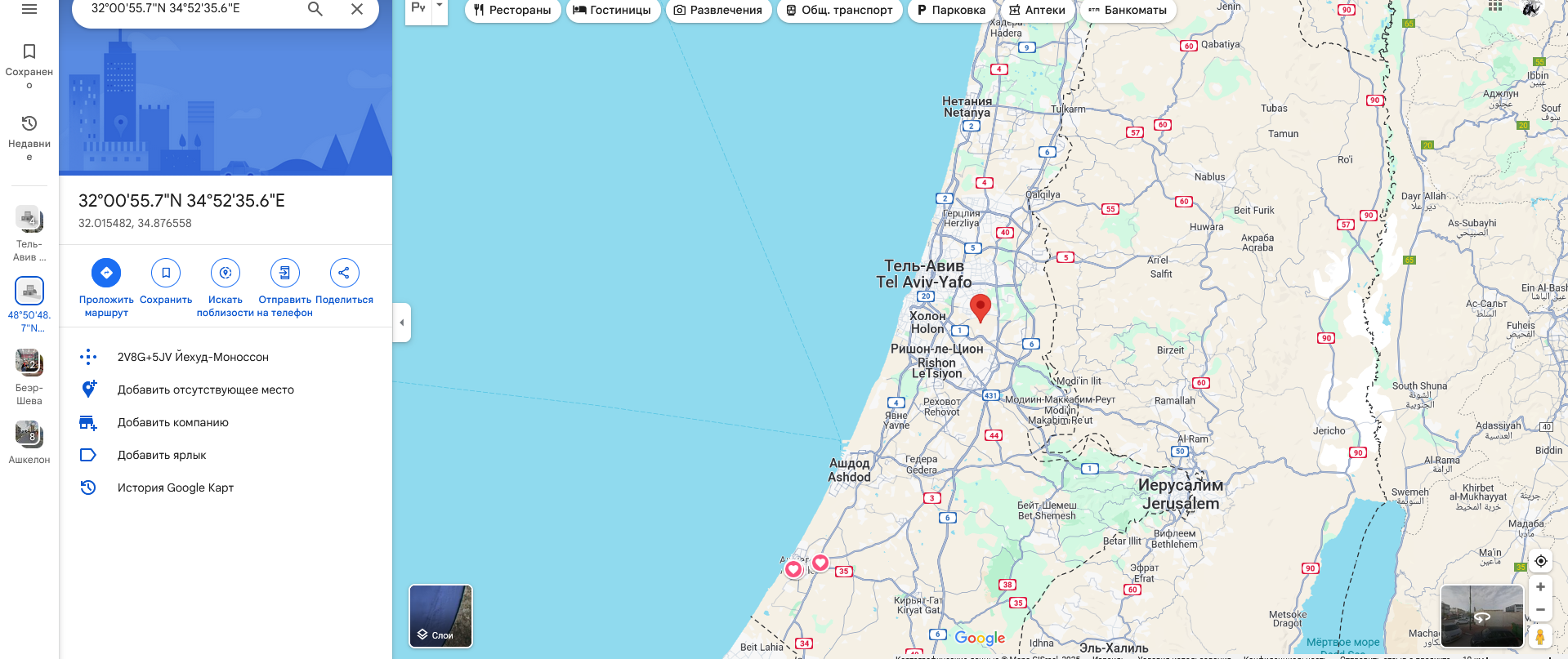
1. מהם המיקומים בהם שהה 0rphan? איפה הוא נמצא כיום לדעתכם?

|  |
| --- |
| המיקומים של 0RPHAN היו קניון רננים,שדה תעופה בן גוריון,פריז,פורט בעיר מרזל,אמצע האוקיינוס ואי ליד צרפת וספרד, לדעתי הוא נמצא באי מהמידע שהסגנו מסעיף 3. |

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



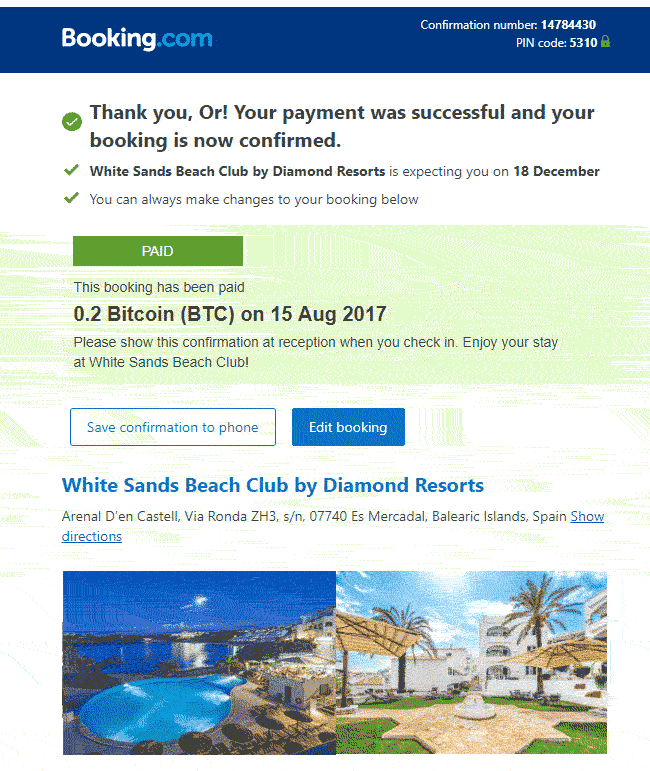




|  |
| --- |
| בש''ב מספר 9, היה כתוב שמיקומו היה בצרפת, בגלל זה הוא היה צרפת, עכשיו כשניסינו להיכנס לחשבונו בבאג, לא הצלחנו לעשות כך, לאחר ההסנפה של האחד הפקטות מצאנו בTCP FOLLOW מצאנו IP חדש שאיתו הלכנו לPUTTY, בPUTTY אנחנו נכנסים לפורט 333 וקולטים כמה פקודות כמו: 20 LOGIN ועלה..., לאחר מכן אנחנו רואים את המסך שבוא יש הרבה GPS ואחד מהם זה המיקום של שדה תעופה של בן גוריון,לאחר מיכן היו את המיקומים האחרים ומכך הבאתי את כול מיקומו הוא היה בהן. |

**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. ****



|  |
| --- |
| שוב פעם עשיתי את אותם פקודות מהסעיף הקודם אך הפעם אחרי פקודת 30 LIST, עשיתי פקודת 40 FILELIST ואז זה נתן לי שם של קובץ בשם booking.gif, וזה אמר לעשות פקודה אחרת ודרך פקודת 40 DOWNLOAD booking.gif זה נותן הרבה טקסט שהוא בעצם base64 code – קוד שאם לפרש אותו לקובץ תמונה דרך אתר\דקודר שיכול לעשות זאת נותן לנו את התמונה הבאה.  אני השתמשתי ב<https://base64.guru/converter/decode/image> |

**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.

|  |
| --- |
|  |