

דו"ח מעבדה - תרחיש מס' 5

פרטים:

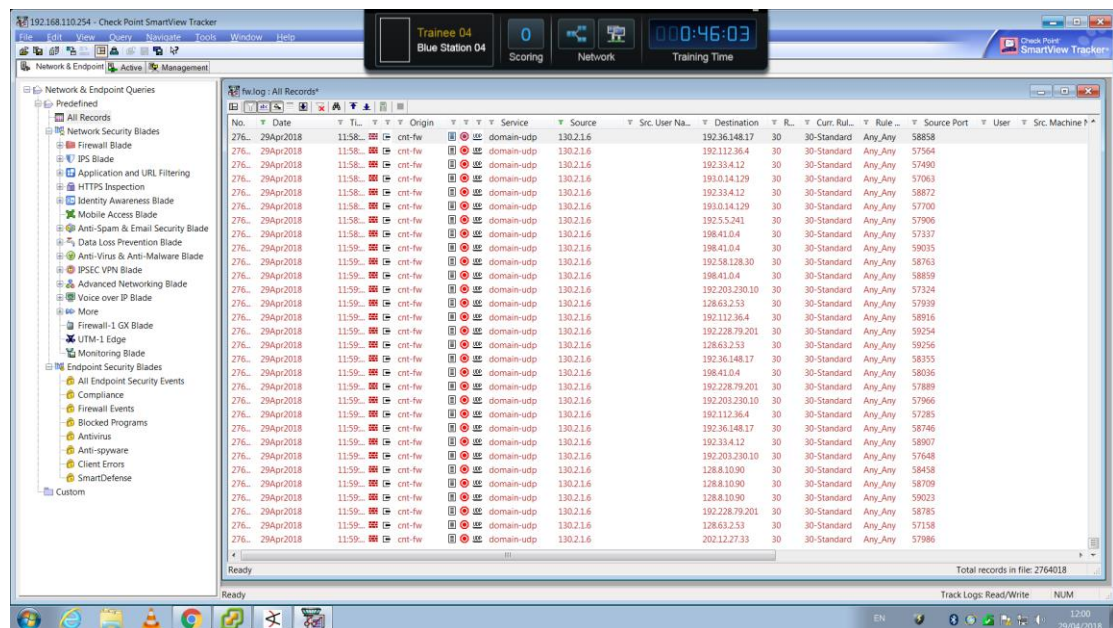
מגיש: שגיא סעדה

תאריך: 29/04/2018

שם התרחיש: מתקפת כופר.

תהליך ההתקפה:

בתהליך ההתקפה זוהו התראות שנשלחות ללא הרף ב- Tracker בפרוטוקול UDP מה- IP הבא: 130.2.1.6 (ה- Firewall בארגון) כל החבילות בסטטוס Drop.
Rule 30 – כל תקשורת שמגיעה עד חוק זה נזרקת, כי היא לא עברה לפי כל החוקים האחרים.



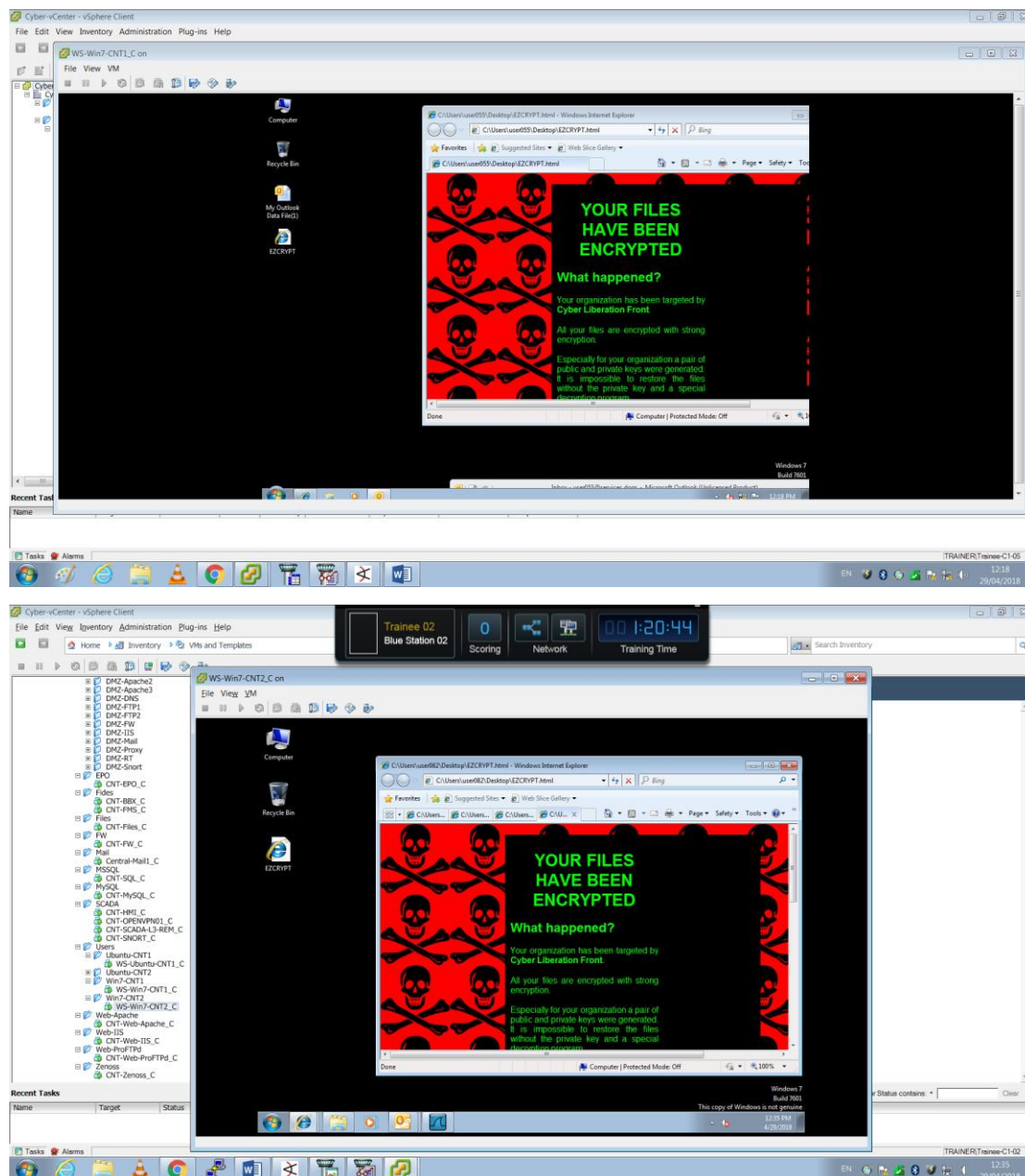
No.	Date	Time	Origin	Service	Source	Destination	Rule	Source Port	User	Src. Machine
276.	29Apr2018	11:58.	cnt-fw	domain-udp	130.2.1.6	192.36.148.17	30-Standard	Any_Any	58858	
276.	29Apr2018	11:58.	cnt-fw	domain-udp	130.2.1.6	192.112.36.4	30-Standard	Any_Any	57564	
276.	29Apr2018	11:58.	cnt-fw	domain-udp	130.2.1.6	192.33.4.12	30-Standard	Any_Any	57490	
276.	29Apr2018	11:58.	cnt-fw	domain-udp	130.2.1.6	193.0.14.129	30-Standard	Any_Any	57063	
276.	29Apr2018	11:58.	cnt-fw	domain-udp	130.2.1.6	192.33.4.12	30-Standard	Any_Any	58872	
276.	29Apr2018	11:58.	cnt-fw	domain-udp	130.2.1.6	193.0.14.129	30-Standard	Any_Any	57700	
276.	29Apr2018	11:58.	cnt-fw	domain-udp	130.2.1.6	192.3.5.241	30-Standard	Any_Any	57996	
276.	29Apr2018	11:58.	cnt-fw	domain-udp	130.2.1.6	198.41.0.4	30-Standard	Any_Any	57337	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	198.41.0.4	30-Standard	Any_Any	59035	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	192.58.128.30	30-Standard	Any_Any	58763	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	198.41.0.4	30-Standard	Any_Any	58859	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	192.203.230.10	30-Standard	Any_Any	57324	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	128.63.2.53	30-Standard	Any_Any	57939	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	192.112.36.4	30-Standard	Any_Any	58616	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	192.228.79.201	30-Standard	Any_Any	59254	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	128.63.2.53	30-Standard	Any_Any	59256	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	192.36.148.17	30-Standard	Any_Any	58355	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	198.41.0.4	30-Standard	Any_Any	58036	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	192.228.79.201	30-Standard	Any_Any	57889	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	192.203.230.10	30-Standard	Any_Any	57966	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	192.112.36.4	30-Standard	Any_Any	57285	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	192.36.148.17	30-Standard	Any_Any	58746	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	192.33.4.12	30-Standard	Any_Any	58907	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	192.203.230.10	30-Standard	Any_Any	57648	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	128.8.10.90	30-Standard	Any_Any	58458	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	128.8.10.90	30-Standard	Any_Any	58709	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	128.8.10.90	30-Standard	Any_Any	59023	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	192.228.79.201	30-Standard	Any_Any	58785	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	128.63.2.53	30-Standard	Any_Any	57158	
276.	29Apr2018	11:59.	cnt-fw	domain-udp	130.2.1.6	202.12.27.33	30-Standard	Any_Any	57986	

בנוסף, ראינו תקשורת המגיעה מחוץ לארגון מה- IP הבא: 199.203.100.100 לעמדת עובד ב- IP הבא: 192.168.100.11.

לאחר כמה דקות התברר שהתקשורת הזאת ישנה, אך למרות זאת, כדאי לבדוק עמדות עובדים בתרחיש התקפה (כמובן שבתרחיש אמיתי העובד יצהיר על כך שהוא תחת התקפה).

תהליך הזיהוי:

בתהליך הזיהוי, התחברנו ל- 4 עמדות העובדים מתוך חשד לתקיפה.



מצאנו שאכן הותקפנו במתקפת כופר (Ransomware) ב- 2 עמדות (CNT1, CNT2). בנוסף, בדקנו את 2 העמדות הנוספות בארגון (ubuntu) ולא מצאנו משהו חשוד.

תוכנת כופר – Ransomware

היא נזקה המגבילה גישה למערכות המחשב הנגוע בדרך מסוימת, ומשתמש לסחוט מהמשתמש תשלום כסף על מנת שתוסר מגבלת הגישה.

חלק מתוכנות הכופר מבצעות הצפנה לקבצים על הכונן הקשיח, ובכך הופכות את תהליך הסרת ההצפנה לקשה מבלי לשלם כופר עבור מפתח ההצפנה, בעוד תוכנות כופר אחרות פשוט נועלות את המערכת ומציגות הודעת שווא כי לא ניתן לגשת לקבצים, על מנת לרמות את המשתמש ולהמריצו לשלם.

לרוב, חודרות תוכנת הכופר למחשב כסוס טרואיני, המוסווה כקובץ תמים.

מקור -

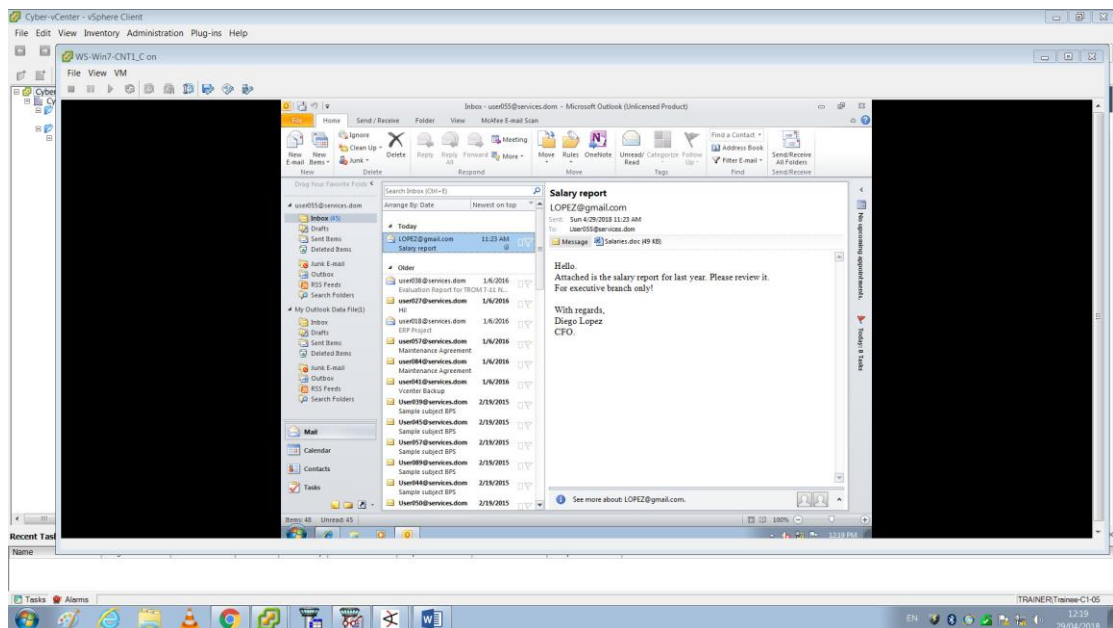
https://he.wikipedia.org/wiki/%D7%AA%D7%95%D7%9B%D7%A0%D7%AA_%D7%9B%D7%95%D7%A4%D7%A8

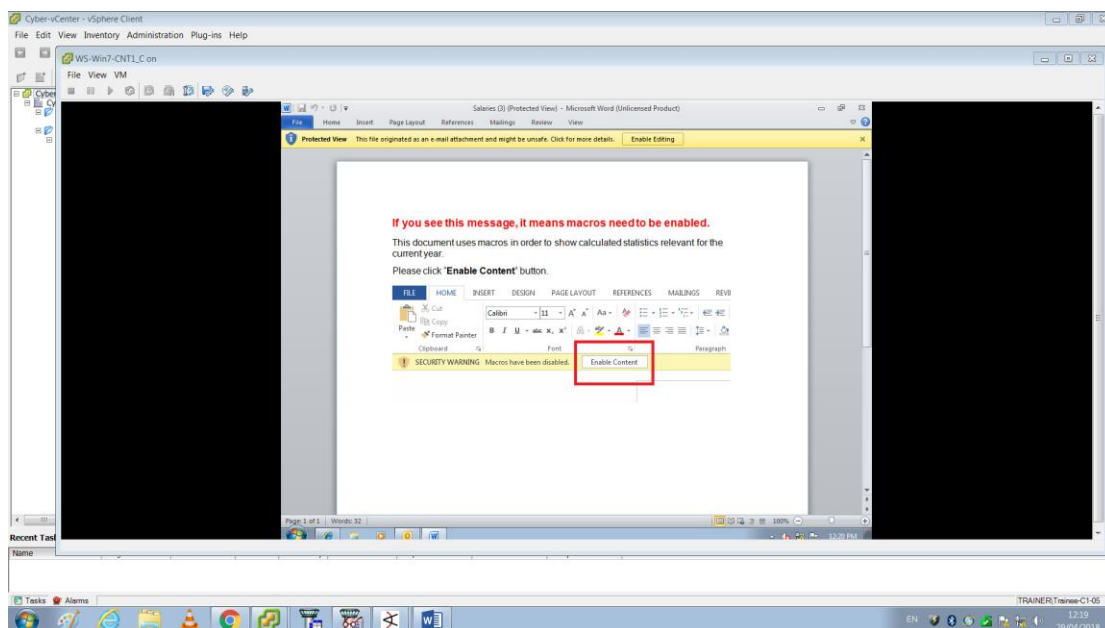
כעת, נעבור לחקירת העמדות –

בשלב זה נרצה לבדוק מה הגורם המרכזי לפריצה, באיזו דרך התהליך קרה ואיך ניתן להתעלות עליו.

מצאנו בדוא"ל של העמדה CNT1 מייל שנראה חשוד – דו"ח משכורת.

כאשר מורידים את הקובץ (קובץ מסוג Word) ופותחים אותו, יש בקשה ללחוץ על Enable editing.





מניסיון של מארק, ניתן להחדיר סקריפטים של Metasploit בצורה זו.

Metasploit – פרויקט מטהספלוית הוא כלי המיועד למבדקי חדירה, מכיל בתוכו מאגר נתונים ופגיעויות נגד מערכות הפעלה, מערכות אנטי וירוס ותוכנות שונות.

ניצול נכון של מידע זה עשוי להוות דלת אחורית להתחברות אל מחשב היעד.

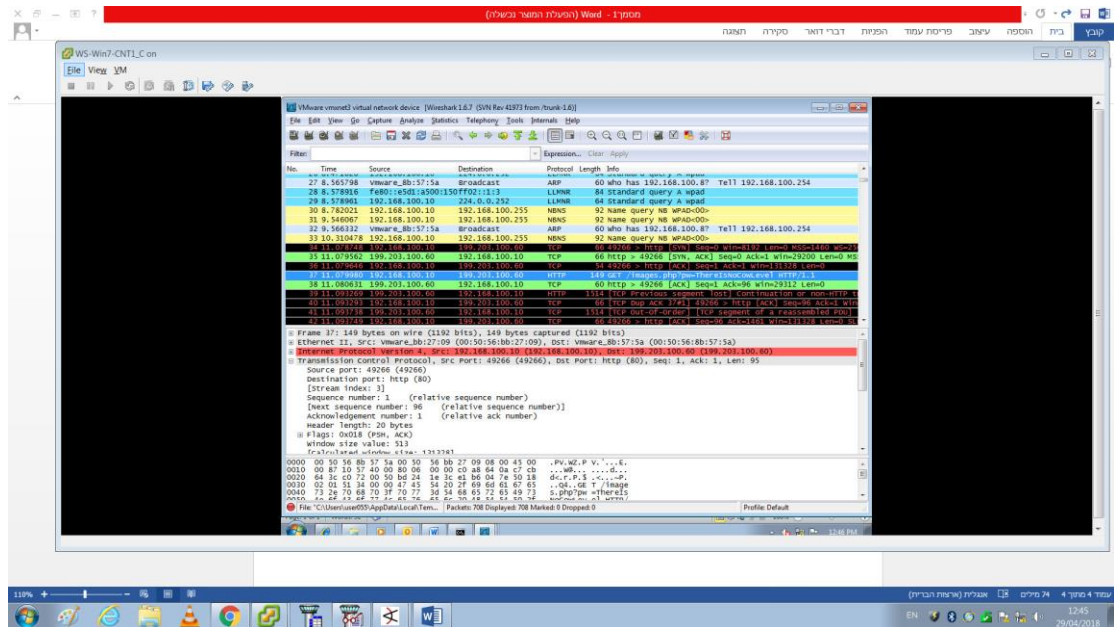
הפרויקט מבוסס קוד פתוח ומקבל תרומות והצעות עריכה מקהילת המשתמשים באמצעות אתר GitHub, ההצעות נבדקות על ידי צוות המורכב מעובדי Rapid7 וחברי קהילה בכירים.

מקור - <https://he.wikipedia.org/wiki/Metasploit>

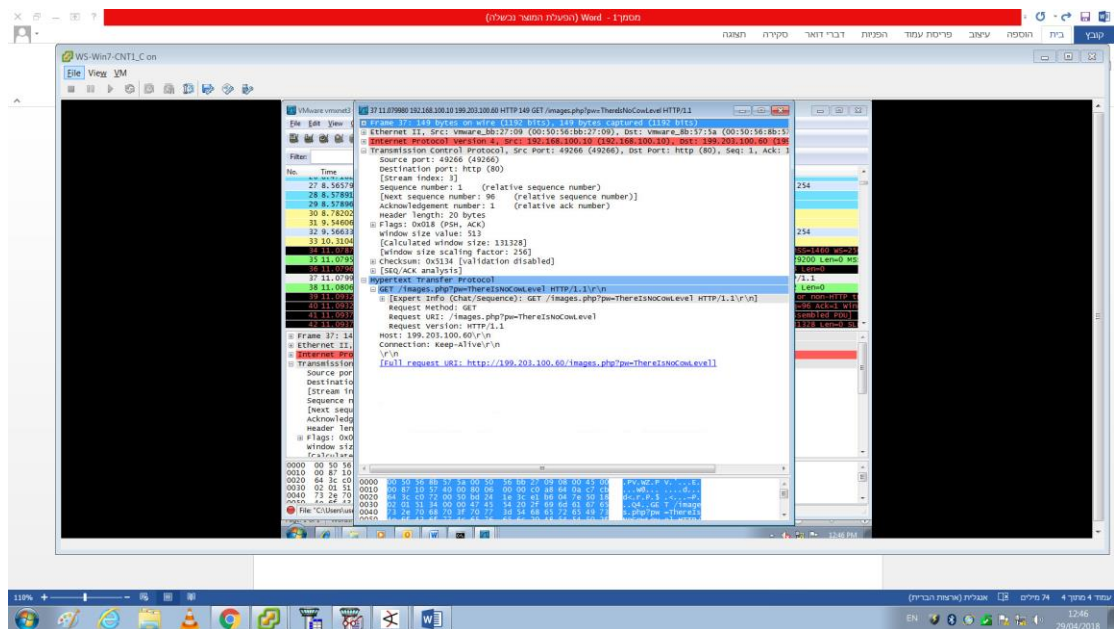
מכאן, ניתן להסיק שככל הנראה עובד לחץ על המייל החשוד והרעיל את העמדה (ואולי עמדות נוספות).

כאשר סוגרים את הקובץ, נוצר קובץ בשם EZCRYPT.html ב- Desktop אשר נפתח בדפדפן ומציג את חלון ההתקפה.

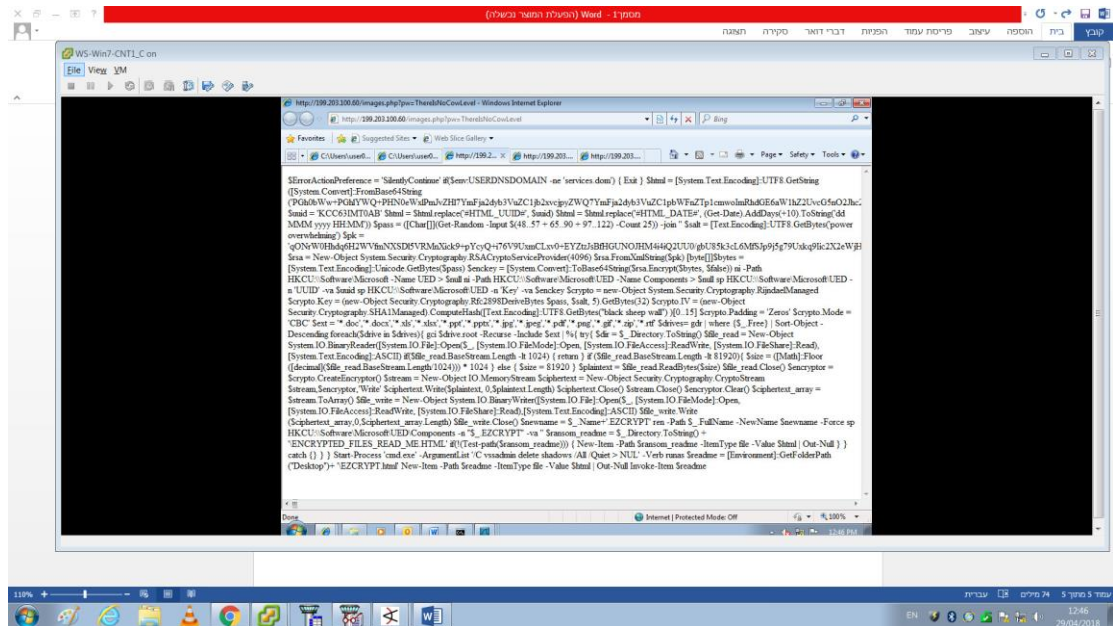
תוך כדי הפעולות הללו הפעלנו Wireshark, ראינו שברגע שלוחצים על הכפתור יש תקשורת TCP עם ה- IP הבא : 199.203.100.60.



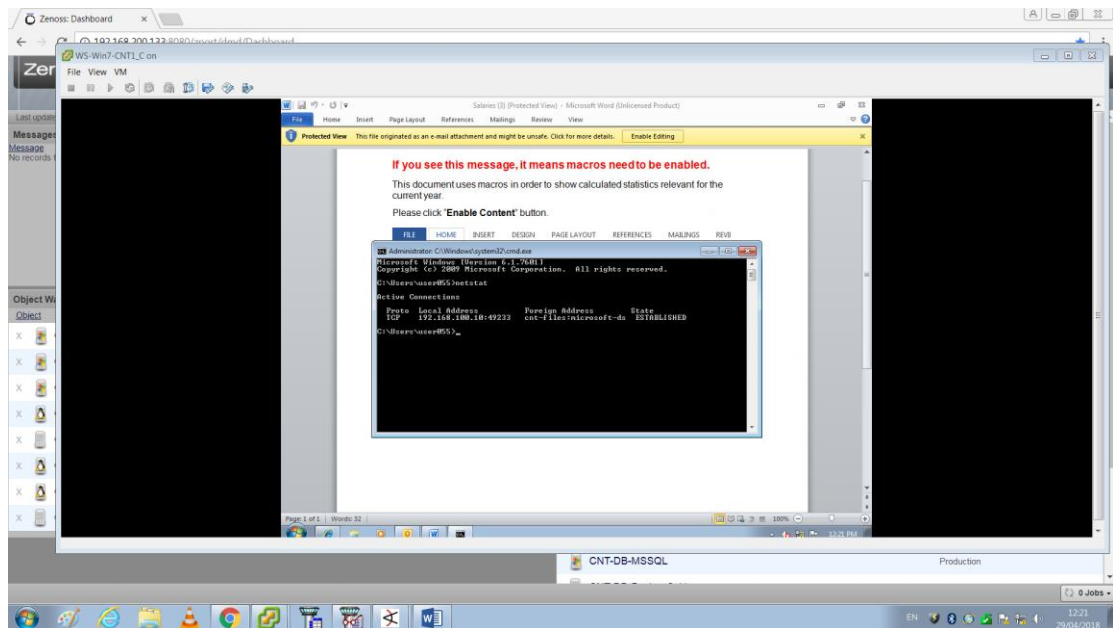
יש פתיחת קשר – לאחר מכן GET לתמונה כלשהי -



פתחנו את הקישור לתמונה וראינו קוד כלשהו, מסתמן - להצפנת קבצים.

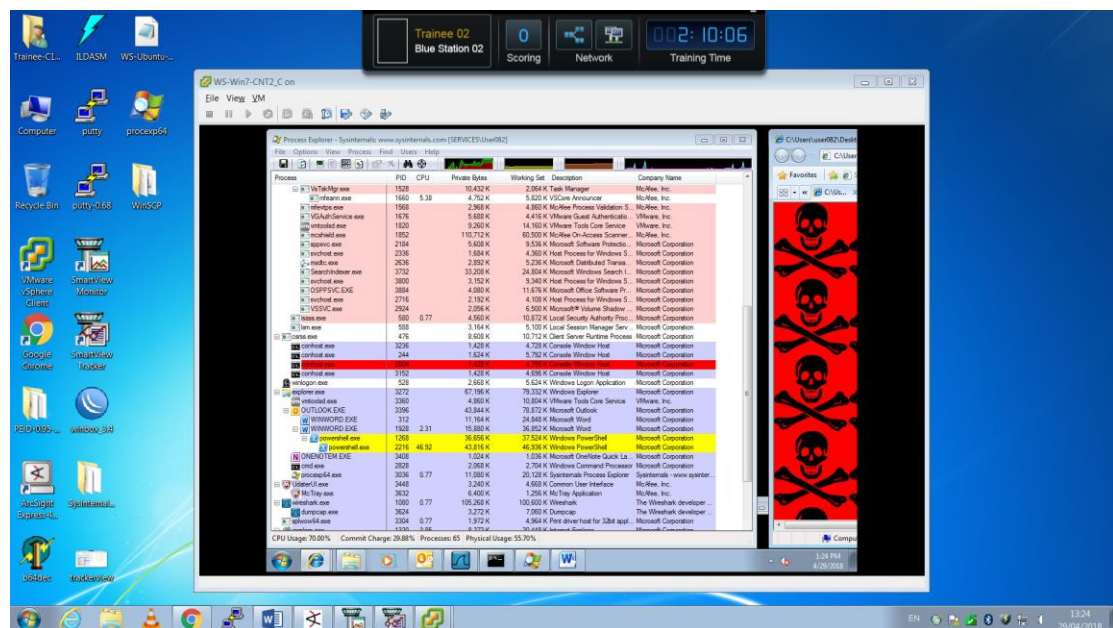
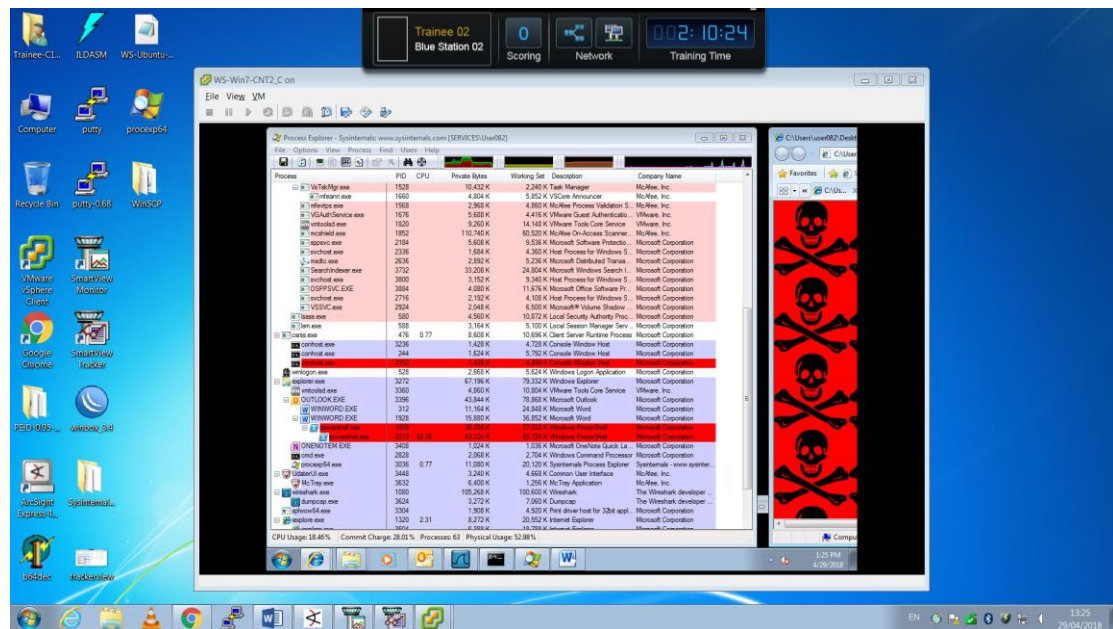


כפי שניתן לראות, הקוד עובר בכל הכוננים במחשב ומצפין קבצים.
בדיקת Netstat על עמדות העובדים –



ניתן לראות חיבור רק לשרת הקבצים של הארגון.

בדיקת תהליכים בזמן אמת בכלי Process Explorer של Sysinternals כאשר לוחצים על הכפתור Enable editing שבזווית הימנית למטה



קפץ תהליך שנעלם לאחר כמה שניות.

Sysinternals – הם אוסף כלים לניהול, אבחון, ניטור ופתרון בעיות בסביבת חלונות מבית מיקרוסופט.
האוסף מכיל כ- 72 כלים ופותח על ידי צוות המפתחים של חברת Winternals.
סוגי כלים –

- ניהול קבצים והדיסק הקשיח
- רשתות
- ניהול תהליכים
- כלי אבטחה
- מידע על המערכת
- תוספות

מקור - <https://he.wikipedia.org/wiki/Sysinternals>

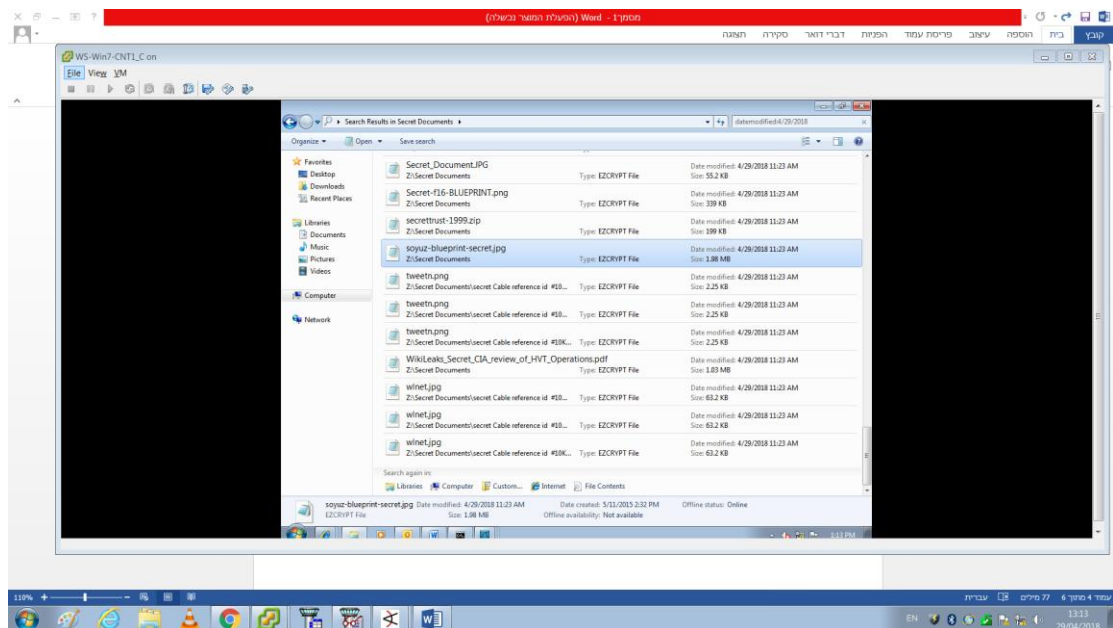
Reverse Shell – סוג תקיפה הגורם לצד הנתקף ליצור תקשורת עם התוקף.

לדוגמא, הנתקף מקבל קובץ זדוני ומריץ אותו.

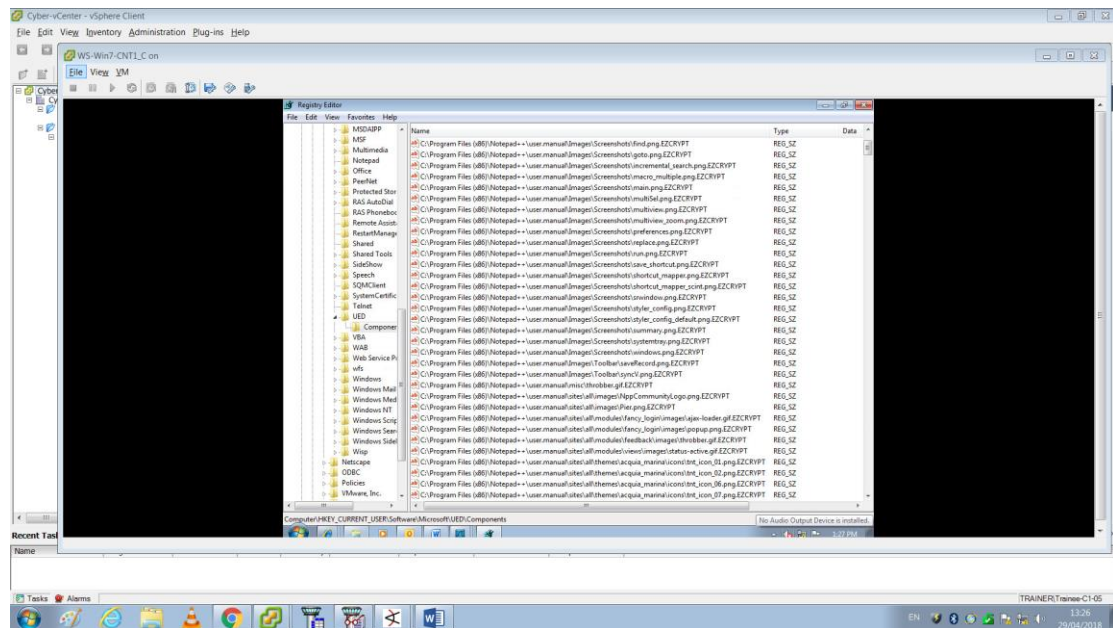
לאחר מכן, מתבצעת יצירת קשר עם התוקף באופן אוטומטי.

כאשר התוקף מאזין לפורט מסוים ברשת שלו, הוא יודע לנהל היטב את הראוטר ברשת זו וכך השיחה של הנתקף תגיע אליו בקלות.

בנוסף, חיפשנו על EZCRYPT ב-Google וראינו שזה כלי חנימי להצפנה ושבירה של קבצים.
מכאן, חיפשנו אילו קבצים הוצפנו בעזרת חיפוש קבצים שעודכנו בזמן שקרה התרחיש ומצאנו



ניתן לראות שהקבצים מסוג EZCRYPT ונמצאים בכונן Z:\ - שרת הקבצים של הארגון.



כמו כן, ראינו שהקבצים ב- 2 העמודות נפגעו מהצפנה.

כעת, עצרנו כדי לחשוב איך ניתן להחזיר את הקבצים לקדמותם ולהסיר את איום התוקף.

ישנם כמה אפשרויות –

- ארגון תקין יבצע שמירת נתונים כגיבוי וכך ימנע איום של מתקפות כופר (אך לצערנו בארגון שלנו אין גיבוי).
- התקפה לצורך הגנה.
- חסימת ה- IP של התוקף ומציאת פענוח לקבצים שהוצפנו. (פענוח יכול לקחת המון זמן)

הגדרת משימות להמשך –

- מארק – אחראי לחפש את המפתח לפענוח ההצפנה ולחפש באתר של התוקף ב- Tor.
- מתן – לחקור כמה רחוק התוקף הגיע בארגון (ב- Subnet 192.168.200.255)
- שגיא – לחקור כמה רחוק התוקף הגיע בארגון (ב- Subnet 172.16.100.255)
- שמואל – לבדוק לוגים של ה- CNT-FW.
- שיר – לחפש קצות חוט בדוק הסקריפט של התוקף, לבדוק לוגים של ה- FW יחד עם שמואל + דו"ח.

מסקנות –

מארק – לא ניתן להגיע למפתח ההצפנה והאתר של התוקף לא קיים.

מתן – התוקף לא הגיע ל- Subnet הנבדק.

שגיא – התוקף לא הגיע ל- Subnet הנבדק.

שמואל – לא נמצאו לוגים חשודים ב- FW.

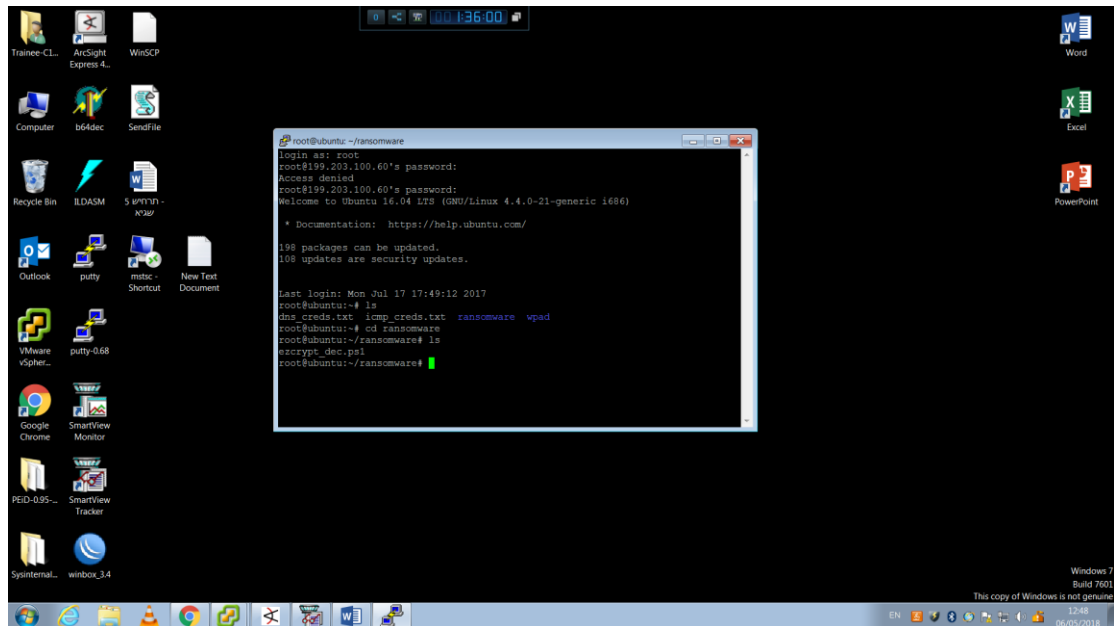
שיר – אין בסקריפט רמזים כלשהם, ואין לוגים ב- FW.

מכאן, מפני שבארגון שלנו לא הצלחנו למצוא גיבוי לקבצים שהוצפנו ולא נתחיל לחפש מפתח לפענוח, נצטרך "לתקוף" את התוקף לצורך הגנה.

ניתן להסיק מכך שלתוקף יש אתר אז פורט 80 פתוח אצלו ולכן,

באמצעות סריקת פורטים של התוקף ניתן לראות שפורט 22 (SSH) פתוח.

לאחר מכן, התחברנו לתוקף באמצעות Putty עם שם המשתמש root וסיסמא P@ssw0rd (שם משתמש וסיסמא נפוצים, באמצעות ניחוש סיסמאות ניתן היה לפרוץ בקלות).

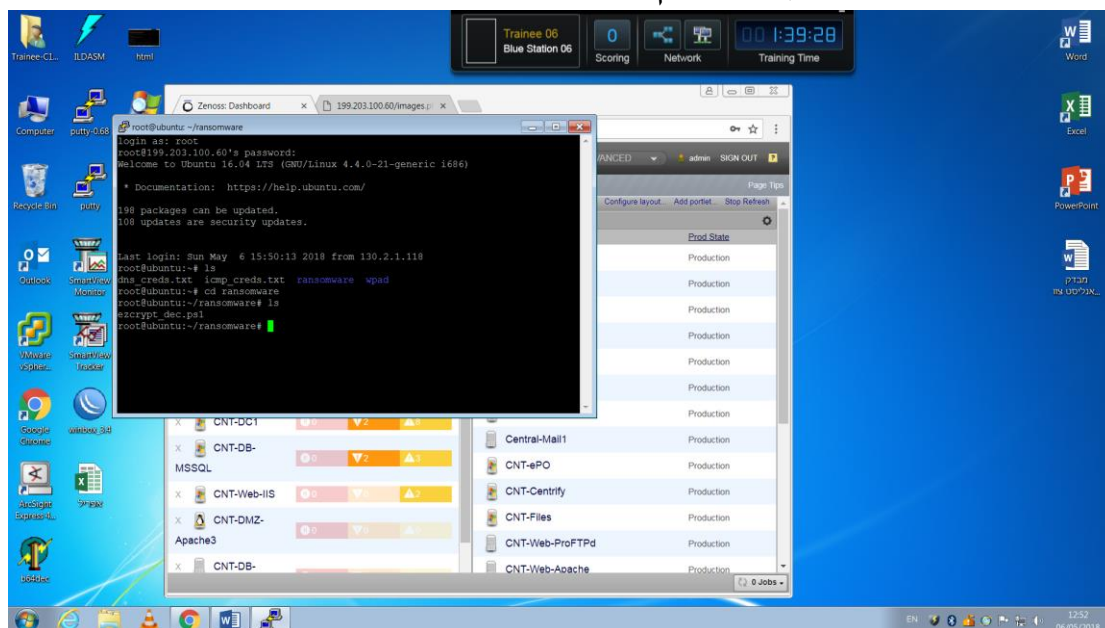


תהליך ההגנה:

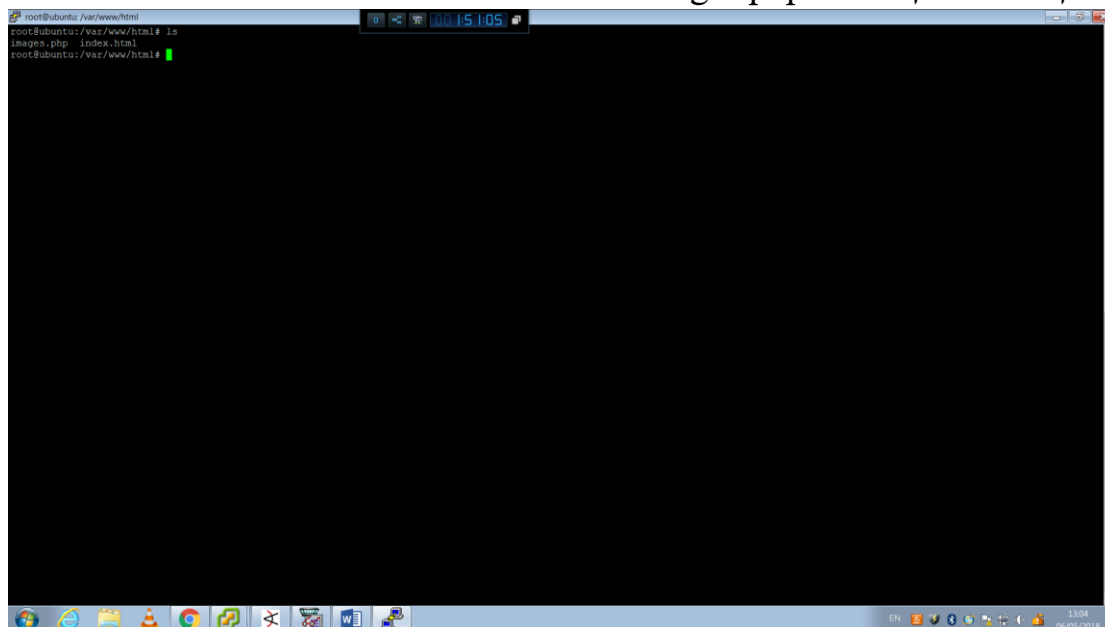
בתהליך ההגנה, לאחר כניסתנו לעמדת התוקף באמצעות SSH נחפש אחר מידע שיכול לעזור לפענח את הקבצים.

התיקיה החשודה הראשונה שמצאנו היא –

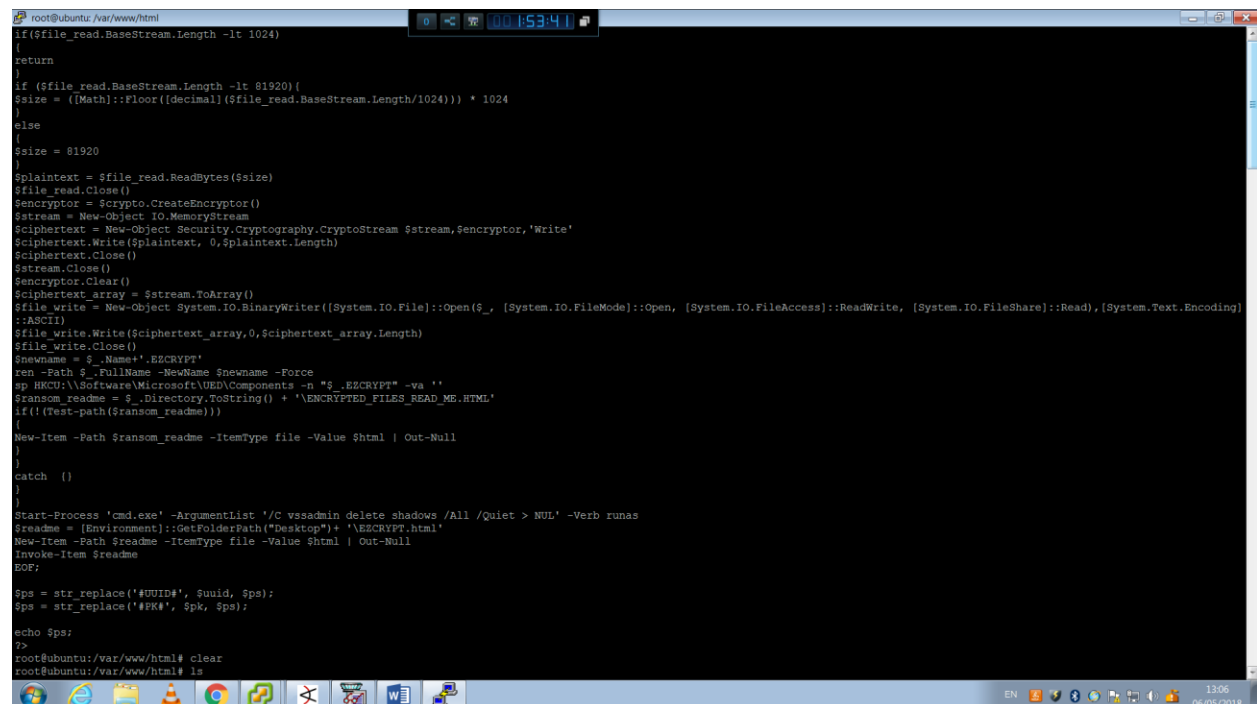
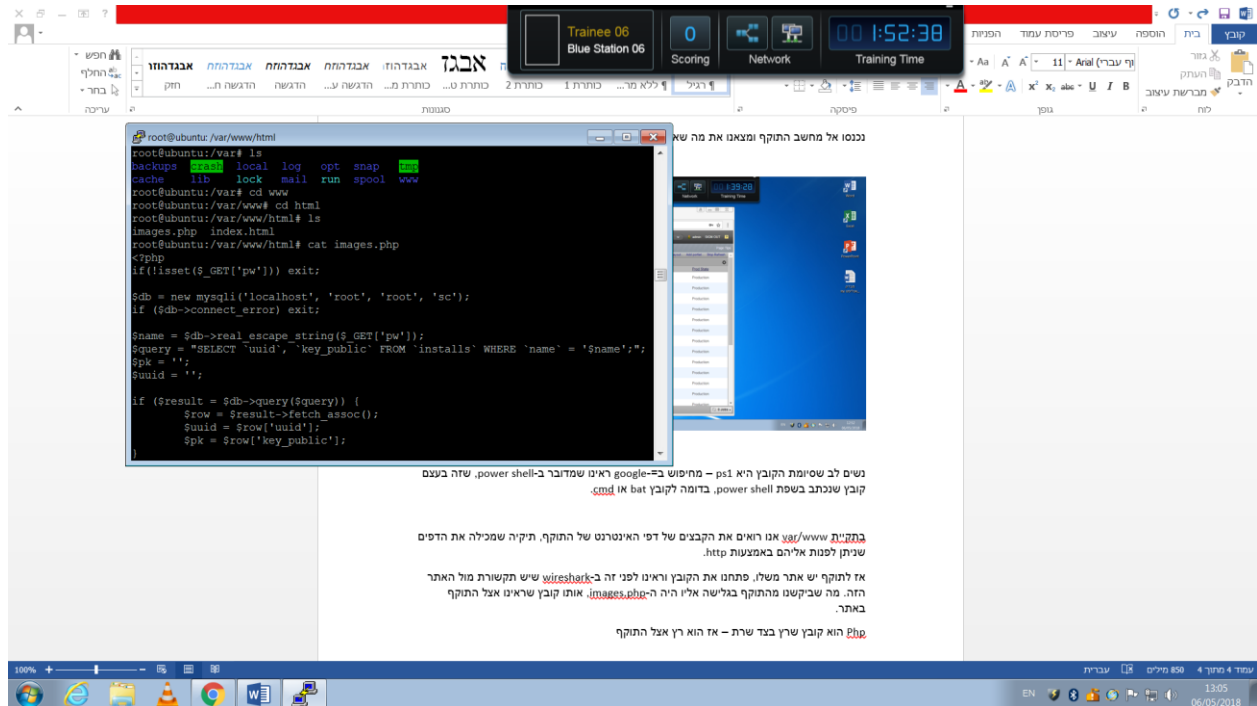
Ransomware המכילה בתוכה קובץ `ezcrypt_dec.ps1` (קובץ PowerShell – נכתב בשפת PowerShell, בדומה לקובץ `bat` או `cmd`).
קובץ זה מבטל את ההצפנה, ואנו רוצים לחפש את המפתח על מנת להזין אותו כך שהקוד ירוץ ויבטל את ההצפנה – יפענח את הקבצים המוצפנים.



ידוע לנו שלתוקף יש אתר – זאת אומרת נחפש קבצים בתיקיה `/var/www/html` ואכן נמצאו הקבצים `images.php` ו-`index.html`



את הקובץ images.php ראינו ב- GET של ה- Wireshark בשיחה בינינו לבין התוקף.
הקוד שיש בקובץ images.php רץ אצל התוקף –



ניתן להסיק שהתוקף משתמש בשאילתה ל- Database אצלו (ב- MySQL) ולכן נרצה להתחבר ל- Database שלו.

עם שם המשתמש root והסיסמא root (לפי נתוני ההתחברות של התוקף המוצגים בקובץ).

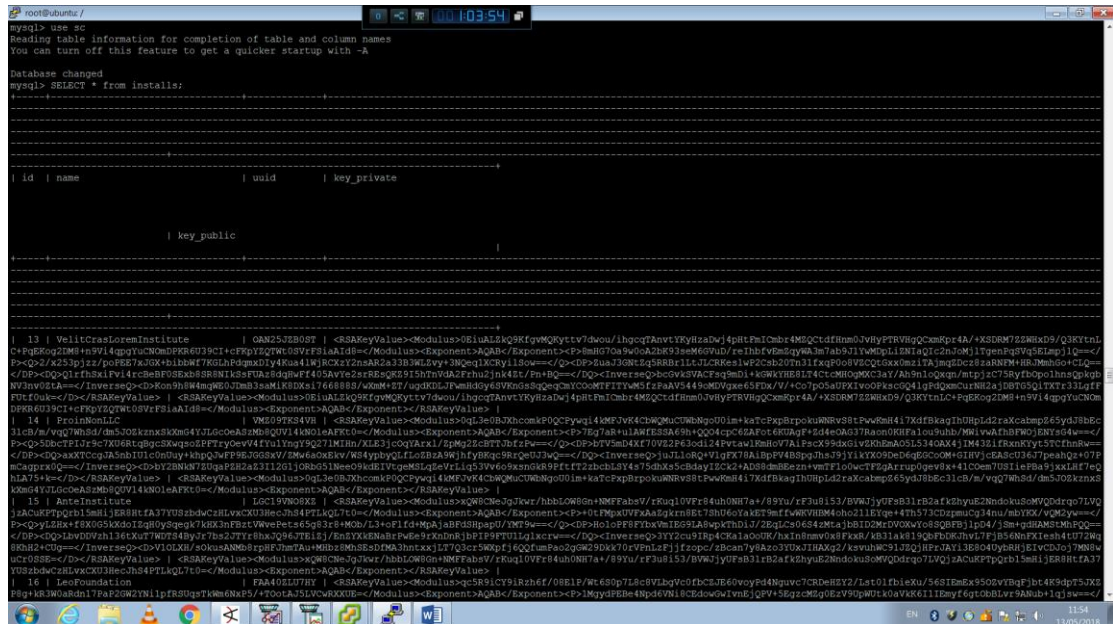
ההתחברות ל- MySQL בלינוקס –

mysql -u root -p

הכנסת הסיסמא root

לאחר מכן התחברות ל- Database עצמו. (בדקנו אילו Databases נמצאים ובחרנו באחד ספציפי – הסבר בהמשך).

use sc



השתמשנו ב- Database sc מכיוון שבדקנו מי מה- Databases מקבל שאילתה עבור 'installs' כפי שהתוקף מבצע בקובץ images.php ורק sc קיבל – ולכן זה ה- Database הרצוי.

(SELECT 'uuid', 'key_public' FROM 'installs' WHERE 'name')

בתהליך זה, נזכרנו שבאתר שנפתח לנו בעמדות המותקפות (עמדות העובדים) יש משפט –

"Your UUID is: KCC63IMT0AB"

Database אצל התוקף.

כך, בעזרת השאילתה –

SELECT uuid name from installs where uuid='KCC63IMT0AB'

```
root@ubuntu: ~  
mysql> select uuid name from installs where uuid='KCC63IMT0AB'  
+-----+  
| name |  
+-----+  
| KCC63IMT0AB |  
+-----+  
1 row in set (0.01 sec)  
  
mysql>
```

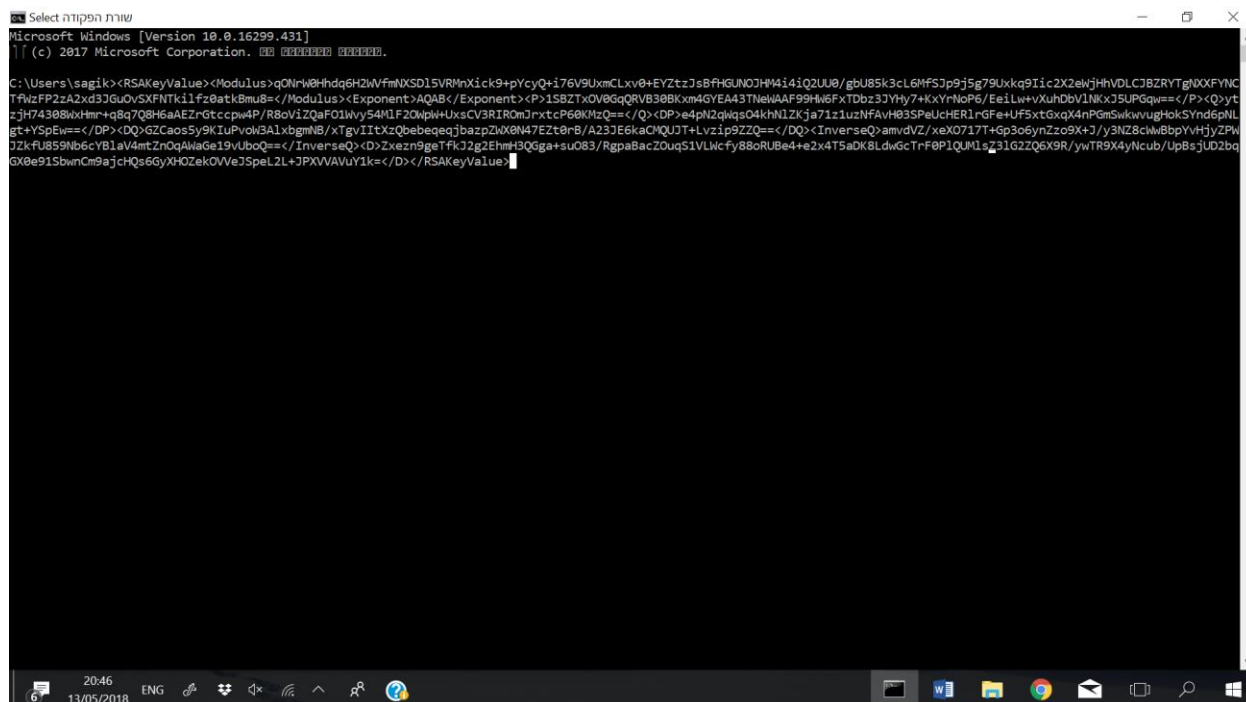
מצאנו את המפתח –

SELECT * from installs where uuid=' KCC63IMT0AB'

```
mysql> select * from installs where uuid=' KCC63IMT0AB'  
+-----+  
| name |  
+-----+  
| KCC63IMT0AB |  
+-----+  
1 row in set (0.01 sec)  
  
mysql> select * from installs where uuid='KCC63IMT0AB'  
+-----+  
| name |  
+-----+  
| KCC63IMT0AB |  
+-----+  
1 row in set (0.00 sec)  
  
mysql>
```

העמקנו בקוד ה- Decryption וראינו שאם נשים בתוכו את המפתח, הוא יפנה לערך ה- Registry ששם הוא שמר את שמות הקבצים שהוא הצפין בתקיפה ולפי רשימה זו הוא יפענח את כולם בהזנת המפתח לקוד.

המפתח אותו נרצה להעתיק לקוד הפענוח –



```
Microsoft Windows [Version 10.0.16299.431]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\sagik><RSAKeyValue><Modulus>qONrW8Hhdq6H2WfmXSD15VRMnXick9+pYcyQ+i76V9UxmCLxv0+EYztzJsBFHGN0JHM4iQ2U0/gbU85k3cL6MfSjP9j5g79Uxkq9Iic2X2elwjHhVdLCJ8ZRYTgWXXFYNC
TFWzFP2zA2xd3JGuOvSXFNTk11fz0atkBmu8=</Modulus><Exponent>AQAB</Exponent><P>1S8ZTxOV8GqQVRB388Kxm4GYEA43TNeWAAF99Hm6FxTDbz3JYhy7+KxYrNoP6/Ee1Lw+vXuhDbV1NKxJ5UPGqw==</P><Q>yT
zjH74388wHmr+q8q7Q8H6aAEZrGtccpw4P/R8oViZQaF01Wvy54M1F20WpW+UxsCV3RIR0mJrxtcP60KHzQ=</Q><DP>e4pN2qHqsO4khN1Zkja71z1uzNFAVH83SPeUcHER1rGFe+Uf5xtGxq4nPgmsWkwvugHokSYnd6pNL
gt+YSpEw==</DP><DQ>GZCaos5y9KIuPvow3A1xbgmNB/xTgviITxzQbebeqejjbazpZwXN47EZt8rB/A23JE6kaCMQUJT+Lvz1p9ZZQ==</DQ><InverseQ>amvdVZ/xeX0717T+gp3o6ynZzo9X+j/y3NZ8clwBbpYVhJyZPW
JZkFU859Nb6cYB1aV4mtZnQaWae19vUboQ=</InverseQ><D>Zxezn9geTfKJ2g2EhmfBQ6ga+su083/RgpaBacZ0uqS1VLWcfy88oRU8e4+e2x4T5aDK8LdwGcTrF8P1QUM1s31G2ZQ6X9R/ywTR9X4yNcub/UpBsJUD2bq
GX0e91SbwnCm9ajcHQs6GyXhOZekOWeJSpeL2L+JPXVAVuY1k=</D></RSAKeyValue>
```

מכאן, נחפש דרך להעביר את קובץ הפענוח לעמדות שהותקפו ובנוסף את המפתח ולאחר מכן נריץ את הקובץ באמצעות Power Shell והקבצים יחסרו לקדמותם.

בשלב זה, הסתבכנו להעתיק את קובץ הסקריפט ps1 לעמדות שהותקפו, ולבסוף הראל מצא לנו פתרון.

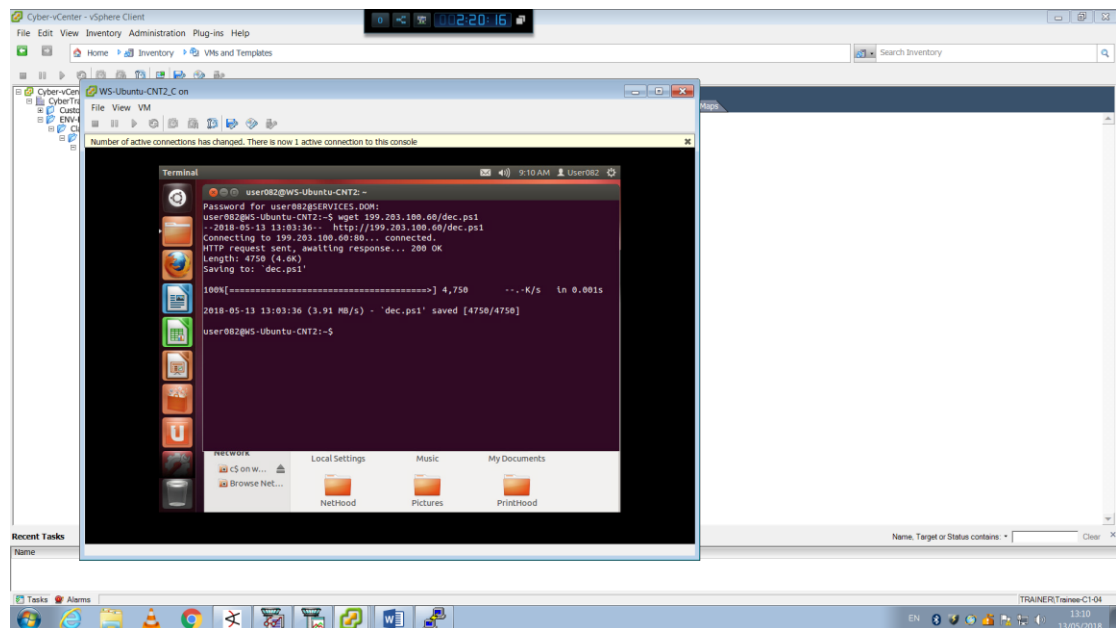
הפתרון הוא –

כאשר שמנו את הקבצים שנרצה להשתמש בהם בתיקייה /var/www/html/ נוכל לגשת אליהם באמצעות כתובת ה-IP של התוקף דרך הדפדפן ובסוף לכתוב את שם הקובץ אליו נרצה לגשת. (דוגמא בתמונה בהמשך).

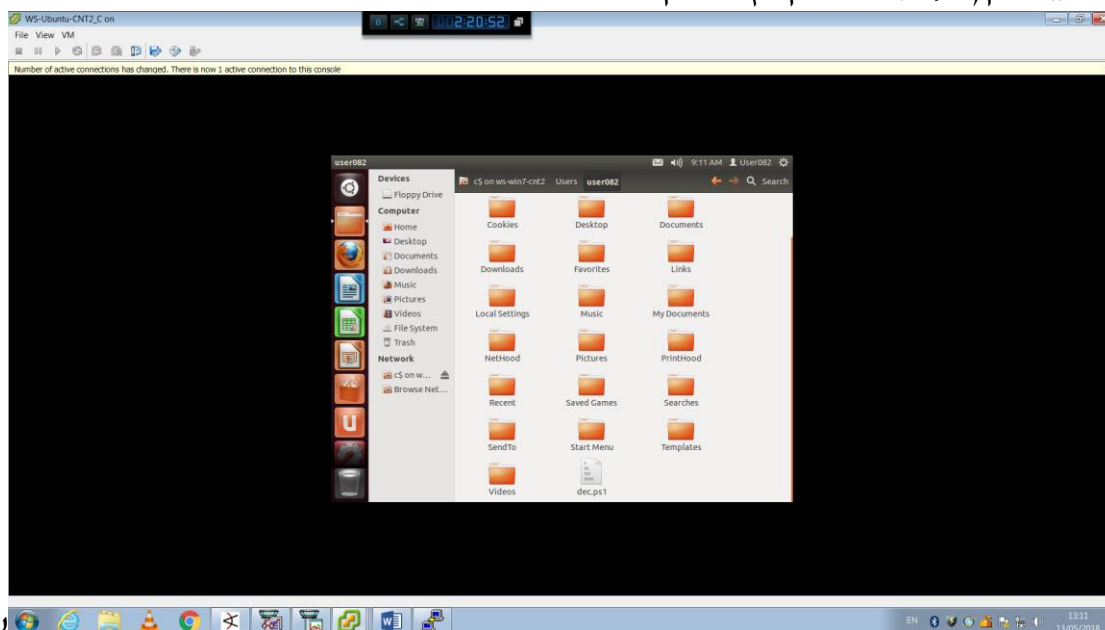
נתחבר לעמדת עובד המשתמש במערכת ההפעלה Ubuntu ובעזרת פקודת wget לקחנו את הקובץ ezcrypt_dec.ps1.

(חשוב לציין שאת הקובץ ezcrypt_dec.ps1 העתקנו לקובץ אחר בעזרת הפקודה –

`cp ezcrypt_dec.ps1 > /var/www/html/dec.ps1`



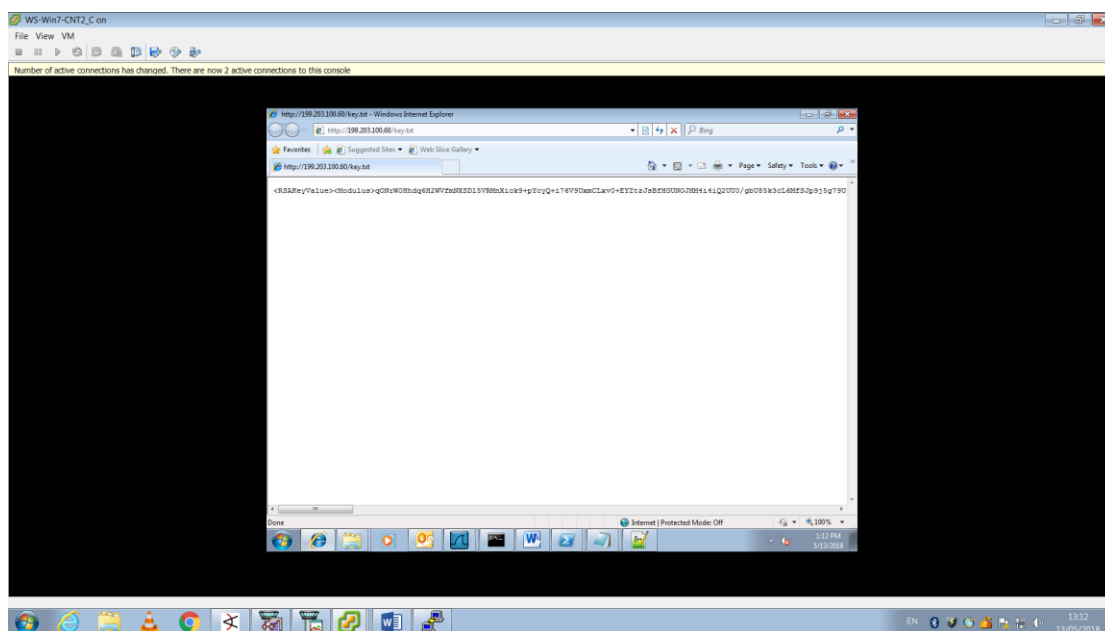
לאחר מכן, נעביר את הקובץ לתיקייה המשותפת user082.



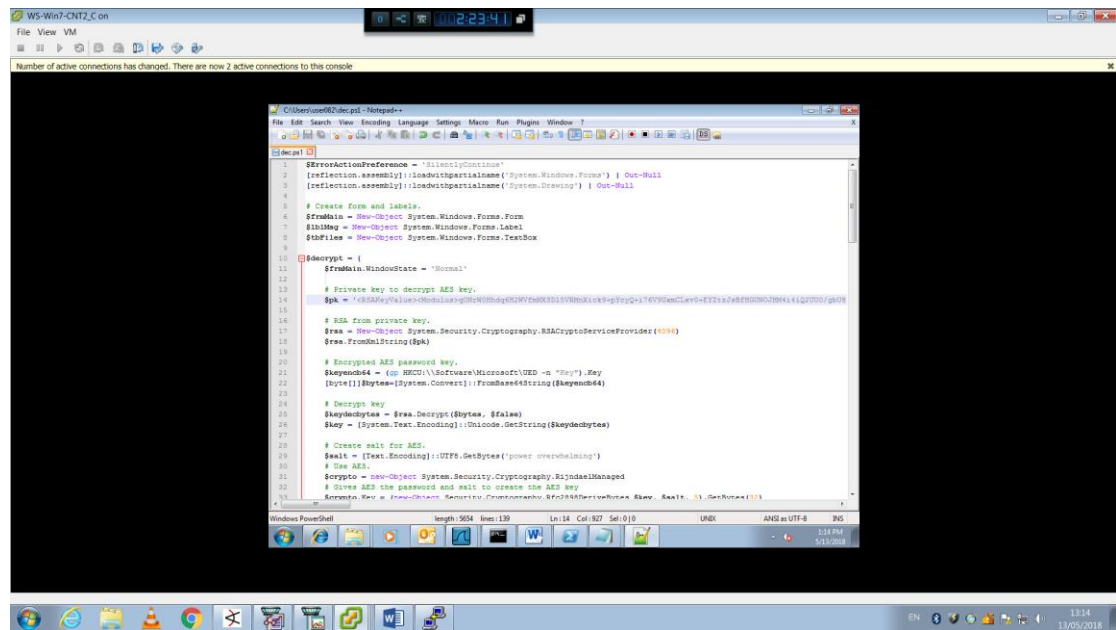
שמנו את

הקובץ בתיקייה המשותפת user082.

בנוסף, בעמדת CNT2 לקחנו את המפתח לפיענוח לאחר שהכנסנו אותו לקובץ key.txt בכתובת /var/www/html/key.txt

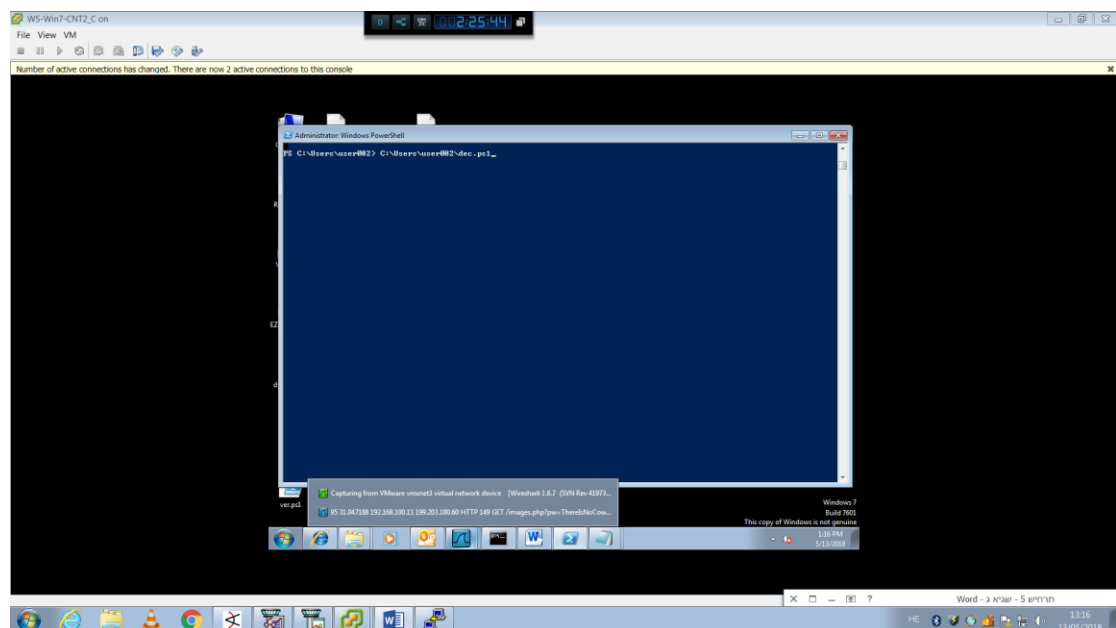


מכאן, הכנסנו את המפתח לקובץ dec.ps1 במקום הערך 'PRIVATE KEY'



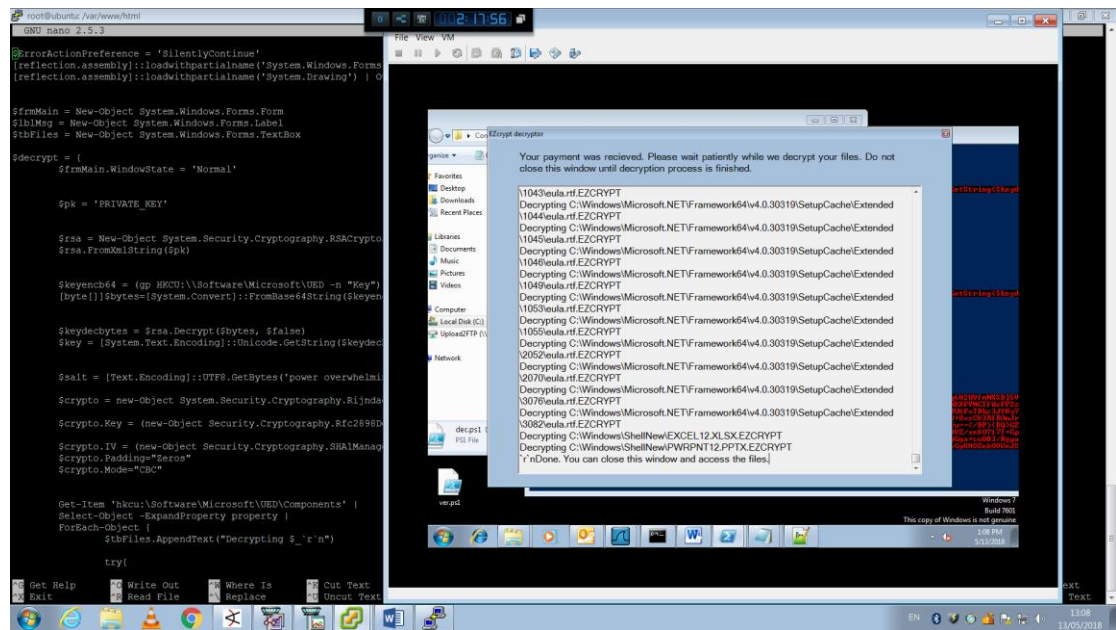
```
1 $ErrorActionPreference = "SilentlyContinue"
2 [reflection.assembly]::loadwithpartialname('System.Windows.Forms') | Out-Null
3 [reflection.assembly]::loadwithpartialname('System.Drawing') | Out-Null
4
5 # Create form and labels.
6 $FormMain = New-Object System.Windows.Forms.Form
7 $lblMsg = New-Object System.Windows.Forms.Label
8 $txtFile = New-Object System.Windows.Forms.TextBox
9
10 # Decrypt
11 $FormMain.WindowState = "Normal"
12
13 # Private key to decrypt AES key.
14 $pk = 'qSMAyqVqUeodAdpLsqrqCW0bBdqG2VYzW0X3D13Y00K1ckg-pcyQ4176Y00enCLeV0+FY112e8f00B070N411q20m/gm'
15
16 # RSA from private key.
17 $rsa = New-Object System.Security.Cryptography.RSACryptoServiceProvider(4096)
18 $rsa.FromBlobString($pk)
19
20 # Encrypted AES password key.
21 $keyencd44 = (gp HKCD\Software\Microsoft\UED -n "Key").Key
22 [byte[]]$bytes=[System.Convert]::FromBase64String($keyencd44)
23
24 # Decrypt key.
25 $keydedbytes = $rsa.Decrypt($bytes, $false)
26 $key = [System.Text.Encoding]::Unicode.GetString($keydedbytes)
27
28 # Create salt for AES.
29 $salt = [Text.Encoding]::UTF8.GetBytes('power overwhelming')
30 # Use AES.
31 $scriptio = New-Object System.Security.Cryptography RijndaelManaged
32 # Give AES the password and salt to create the AES key
33 $scriptio.Key = [System.Security.Cryptography.RijndaelManaged]::New($key, $salt, 32, GetRandomBytes(16))
```

ונרץ את הקובץ ב- Power Shell



```
PS C:\Users\user002> C:\Users\user002\dec.ps1
```


ותהליך הפענוח מתחיל –



תהליך הגנה מונעת :

בתהליך זה יש כמה דברים שכדאי לעשות בארגון כדי למנוע תקיפה מסוג זה –

- 1 – תדרוך העובדים בארגון – לעשות מדי פעם תרחישי תקיפה ולראות איך יגיבו העובדים ומשם להסיק מסקנות שיעזרו בהמשך (כמובן, אזהרות מפני מתקפות מסוג זה).
- 2 – אנטי וירוס בעמדות העובדים שיבדוק את הקבצים שהורדו למחשב (לדוגמא, הכלי RansomFree של Cybereason, ברגע שהכלי מזהה שתוכנת כופר מנסה להצפין קבצים, היא מפסיקה מיד את פעולתה לפני שהקבצים הופכים למוצפנים ומתריעה על כך מפני המשתמש).
- 3 – מערכת הגנה עבור דוא"ל (אנטי וירוס שסורק את הדוא"ל) – כל דוא"ל צריך לעבור סינון כלשהו אם זה על ידי האדם המקבל או על ידי מערכת אוטומטית. לדוגמא, אם הדוא"ל שנשלח מצורף עם קבצים, על המערכת לבדוק את הקבצים קודם לכן בעזרת הורדה למקום שמור ולעדכן במידה והקבצים זדוניים (מומלץ לחסום קבצי EXE או SCR).
- 4 – יש לבצע גיבויים (מומלץ גיבוי אונליין ולא מקומי) מדי שבוע (פחות או יותר) של מידע חשוב בשרתים ובעמדות העובדים וכמובן לבצע בדיקה תקופתית של שחזור הגיבויים כדי לוודא שהם תקינים.
- 5 – יש לשמור על מערכת הפעלה, תוכנות ואפליקציות מעודכנות – ישנם פרצות אבטחה ידועות במוצרי תוכנה ומצליחים באמצעותם לחדור למחשבים בקלות. כאשר מתגלה פרצה בתוכנה כלשהי, לרוב היצרן דואג להפיץ תיקון (באמצעות עדכון), אך כל עוד התוכנה המותקנת במחשב לא עודכנה, הפרצה עדיין קיימת.

הפרצות באבטחת הארגון

ראה סעיף "תהליך הגנה מונעת"

ובנוסף, הארגון מאפשר לעובדים לגשת לשרת הקבצים הפנימי באופן פשוט מדי, מומלץ לאפשר פעולה זו על ידי סיסמא כך שבמידה והמחשב נפרץ, רק העמדה עצמה נפגעת.

כלים שפיתחנו

אין ברשותנו כרגע את הידע לפתח כלים.

אופן עבודת הצוות

בתרחיש זה, התקיפה הייתה רחבה יותר מתרחישים קודמים (2 עמדות ושרת הקבצים נפגעו בתקיפת כופר שמובילה להצפנת הקבצים).

לכן, חילקנו את העבודה בין כולם וכך תהליך ההגנה והפענוח היה יעיל יותר.

שמואל – חקירת ה-FW של הארגון. (בדיקת לוגים)

מתן ומארק - התחברות לעמדות שהותקפו וחקירתן (חקירת עמדה).

שגיא - התחברות לשרת הקבצים וחקירתו (חיפוש גיבוי מידע).

יצחק – חקירת היקף הפגיעה בארגון.

שיר – כתיבת דו"ח ומציאת פתרונות להתקפות כופר.

חוסרים/קשיים

זאת פעם ראשונה שהתמודדנו עם סוג של התקפה מהצד שלנו, היינו צריכים לתקוף את התוקף ולשאוב ממנו מידע הנחוץ לפענוח הקבצים ולכן התעכבנו בפתרון התרחיש.