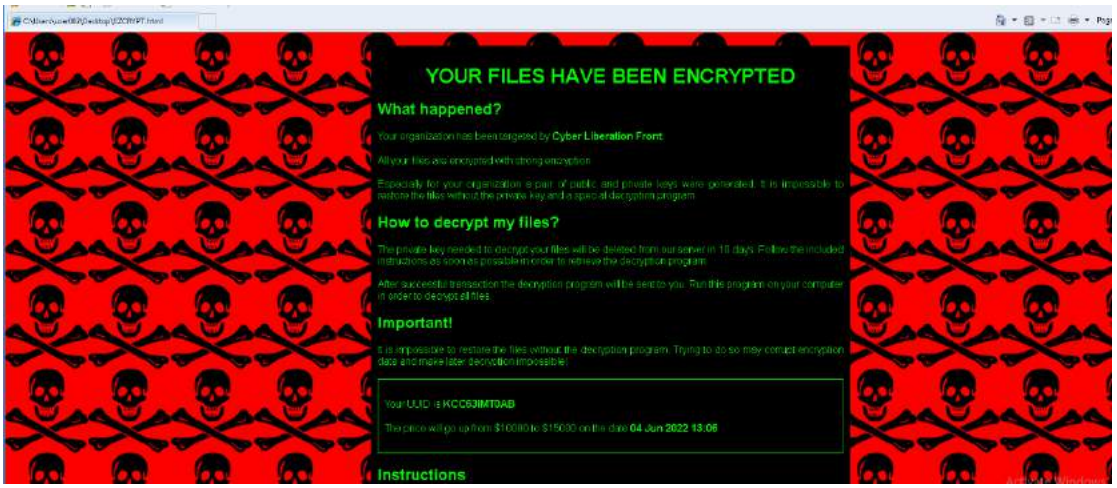
בתדרוך המשימה שלנו נכתב שאחד המחשבים (שמו WS-Win7-CNT2) ברשת שלנו התלונן שהמחשב שלו מתנהג מוזר (acting weird)

Welcome aboard!
You are a member of the SOC team. Your shift has just begun.
One of your organization's employees who uses the "WS-Win7-CNT2" computer, called to complain that his computer is "acting weird".
You need to detect, analyze, and report every step of the attack using the investigation tool.
Examine the network using the tools provided (see the instructions that follow).
When you are done discovering and have confirmed the source of the attack, the authorities will bring you the CNC server for investigation. The CNC credentials are:

בדקנו איזו מערכת הפעלה יש במחשב הזה והתחברנו אליו

| | NAME | MACHINE NAME | DESCRIPTION | OPERATING SYSTEM | IP |
|---|---|---|---|---|---|
| | Windows 7 Workstation | WS-Win7-Cnt1 | Windows 7 Workstation | Windows 7 Pro | 192.168.100.10 |
| | Windows 7 Workstation | WS-Win7-Cnt2 | Windows 7 Workstation | Windows 7 Pro | 192.168.100.11 |
| | Windows 10 Workstation | WS-Win10-CNT1 | Windows 10 Workstation | Windows 10 Ent | 192.168.100.12 |
| | Windows 10 Workstation | WS-Win10-CNT2 | Windows 10 Workstation | Windows 10 Ent | 192.168.100.13 |

ראינו חלון בו היה כתוב שהקבצים שלנו מוצפנים וכדי להחזיר אותם צריך לשלם 10,000-15,000 דולר




בדרך כלל, וירוסים להדביק את המחשב של הקורבן, ולאחר מכן הם יכולים לעבוד במצב שינה ללא כל תופעות לוואי עבור מערכת ההפעלה. ורק וירוס אחד פועל מיד על המצח: זוהי תוכנית סחיטה ransomware (הדוגמאות המפורסמות ביותר של "וירוס פטיה" ו BadRabbit). עם זאת, זה סוג זה של וירוסים הפך ביותר "פופולרי" בשנת 2017. התוקפים משתמשים ב-ransomware מכמה סיבות:

וירוס ransomware כזה מדביק את המחשב די מהר;

העבודה של וירוס כזה אינו נדרש לשמור: הוא מופעל פעם אחת, ולאחר מכן הוא יכול אפילו לכבות – העבודה השחורה שלו כבר נעשה;

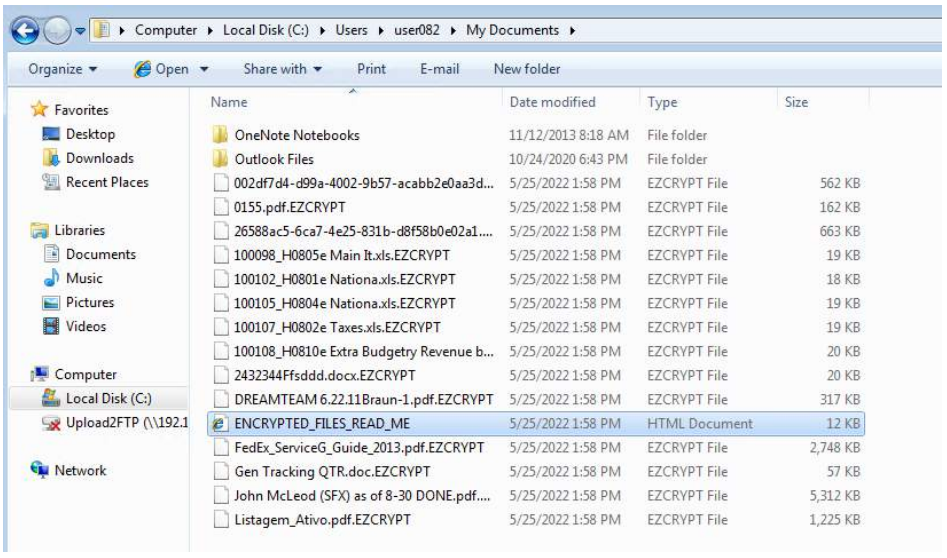
באמצעות ransomware, קל מאוד להשיג תגמול כספי-הכל בגלל שהווירוס מפריע לעבודה ו/או מצפין נתונים חשובים שמשתמשים לא רוצים להפסיד.

Ransomware, מצפין קבצים - הן במערכת והן בנתונים אישיים. בדרך כלל, בתוך כל תיקיה מוצפנת, ניתן למצוא את קובץ ה-readme, שבו נכתב ההוראה "להציל" את הנתונים. הווירוסים הידועים ביותר של מין זה נקראים wannacry ו-Petya

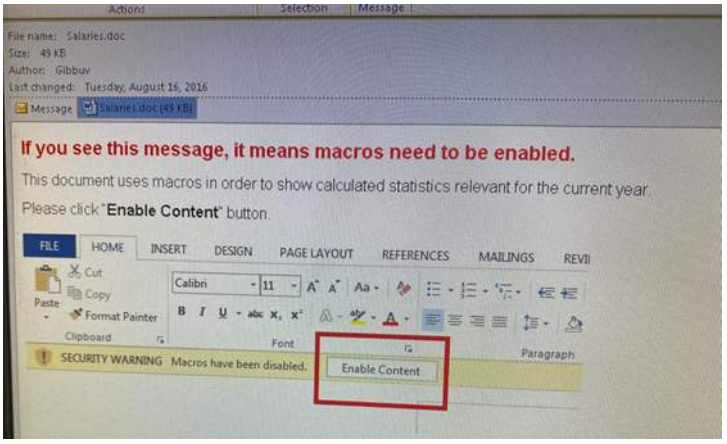
החוסם באופן מלא או חלקי את העבודה במערכת ההפעלה. בדרך כלל החסימה באה לידי ביטוי Ransomware בחלונות קופצים המופיעים מדי פעם עם מודעות או שיחות לשלם כסף. חלונות כאלה הם לעתים קרובות בלתי אפשרי למזער בפעם הראשונה

החוסם באופן מלא או חלקי את העבודה בדפדפן. כאן העיקרון הוא בדיוק כמו בנקודה שתיים, עם Ransomware ההבדל היחיד שחלונות מפריעים לעבודה רק בדפדפן האינטרנט. אותה נקודה כוללת וירוסים המפיקים מודעות בדפי אינטרנט.

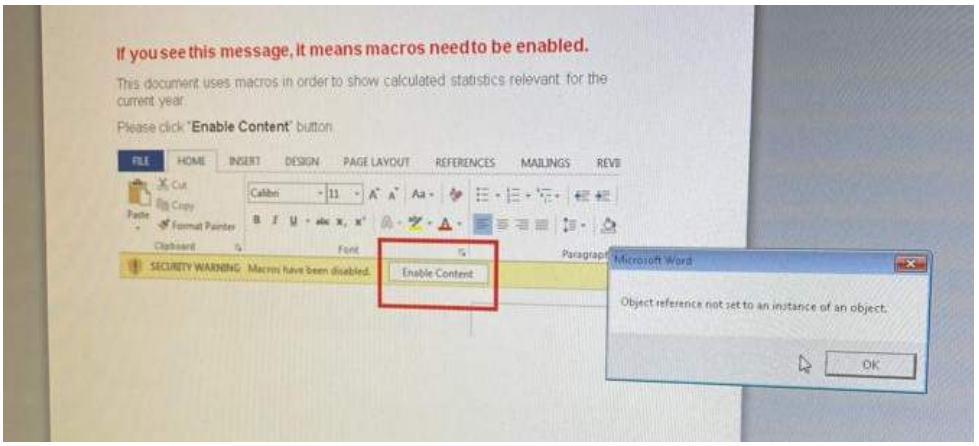
בתיקיות ראינו הרבה קבצים עם הסיומת EZCRYPT. המערכת עדיין פעלה, אז הגענו למסקנה שרק קבצים שלא השפיעו על פעולת המערכת הוצפנו. ליתר דיוק, מסמכים. ראינו גם באיזו שעה השתנו הקבצים (5.25 ב 1:58pm)



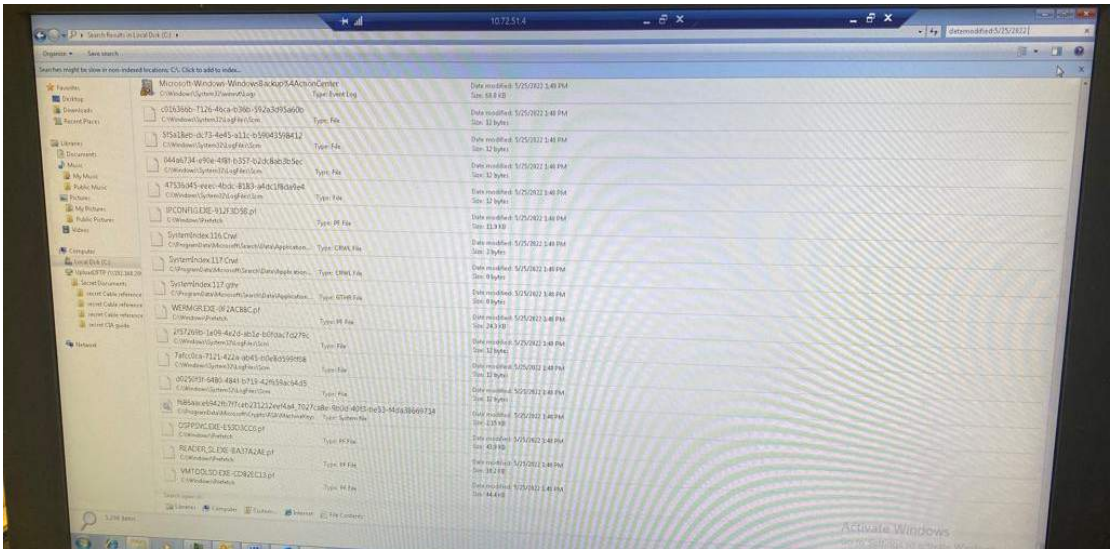

הלכנו לתיבת הדואר של המשתמש הזה וראינו שבשעה 13:53 הוא קיבל מייל מלואיס והיה גם קובץ מצורף



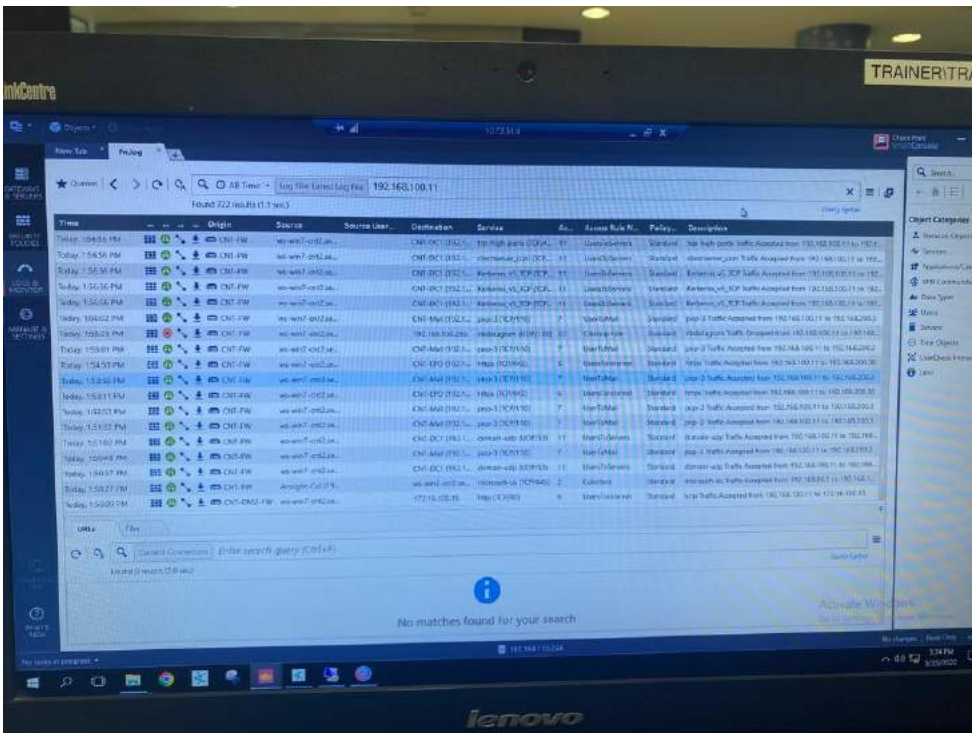

הורדתם והפעלתם את הקובץ הזה



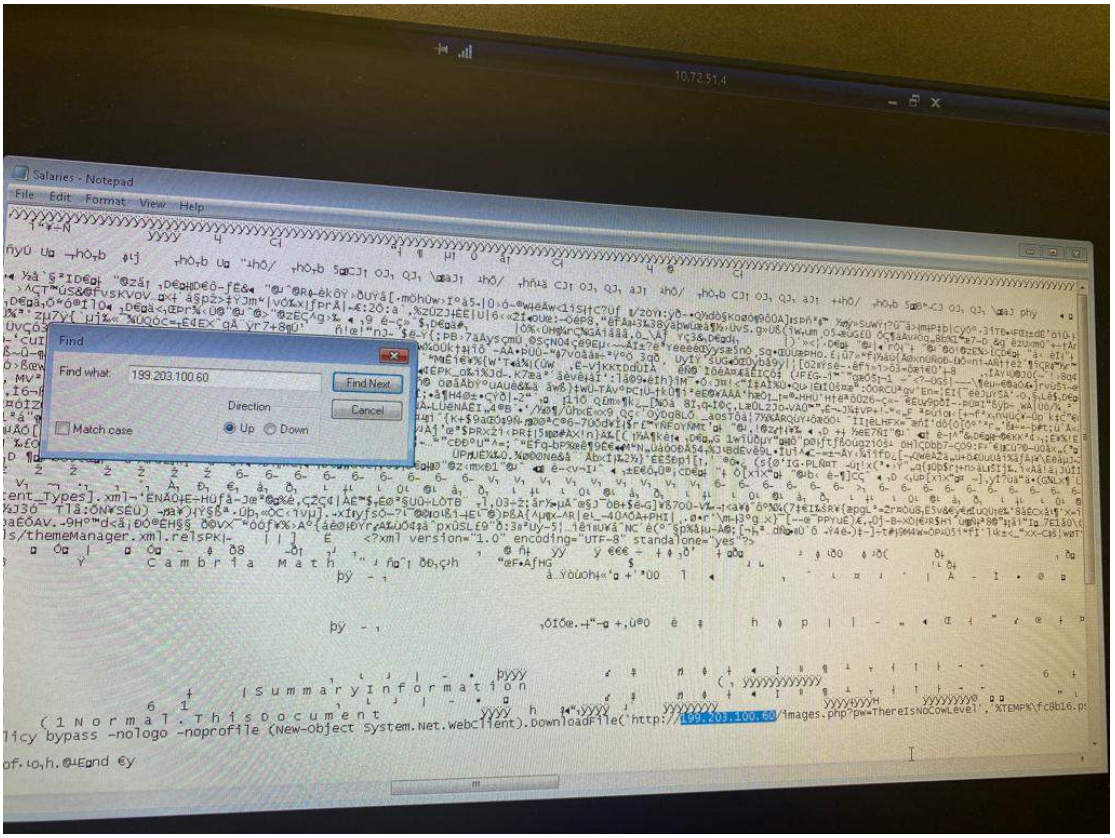

הבנו שסקריפט כלשהו מותקן במחשב והחלטנו למצוא את הקבצים ששונו אחרונים



הכנסנו גם את הכתובת של המחשב הנגוע שלנו לתוך המסנן בחומת האש



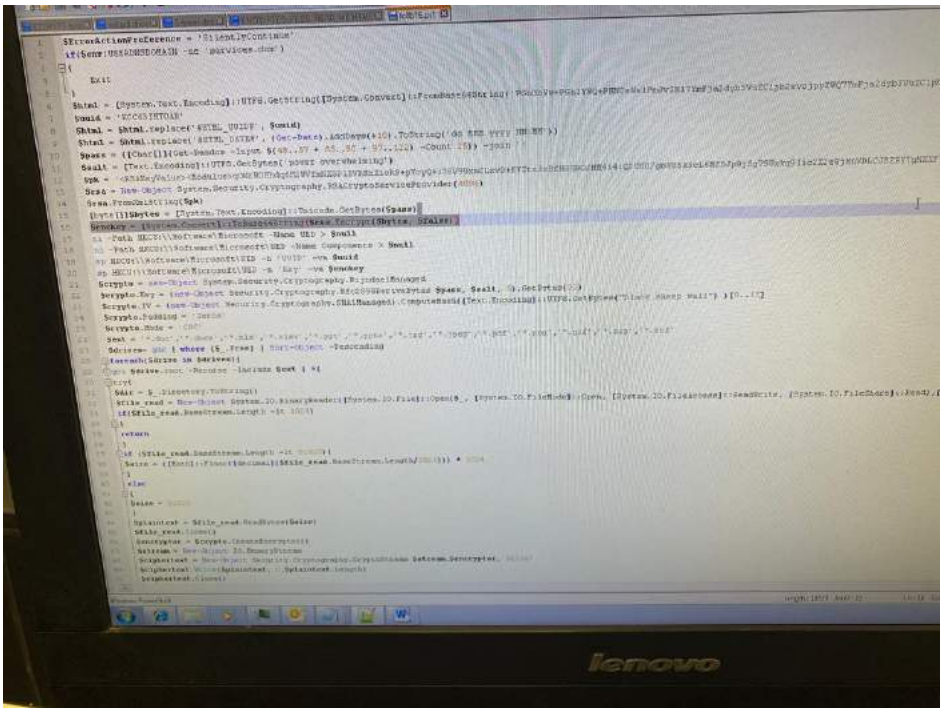

בחיפוש בתוך הקובץ שהיה בדואר של העובד שלנו, כתבנו את הכתובת החיצונית שנמצאה קודם לכן




אז מצאנו את התסריט

בתוך הסקריפט, קראנו שנוצר קובץ זמני temp.

מצאנו ופתחנו את הקובץ הזה

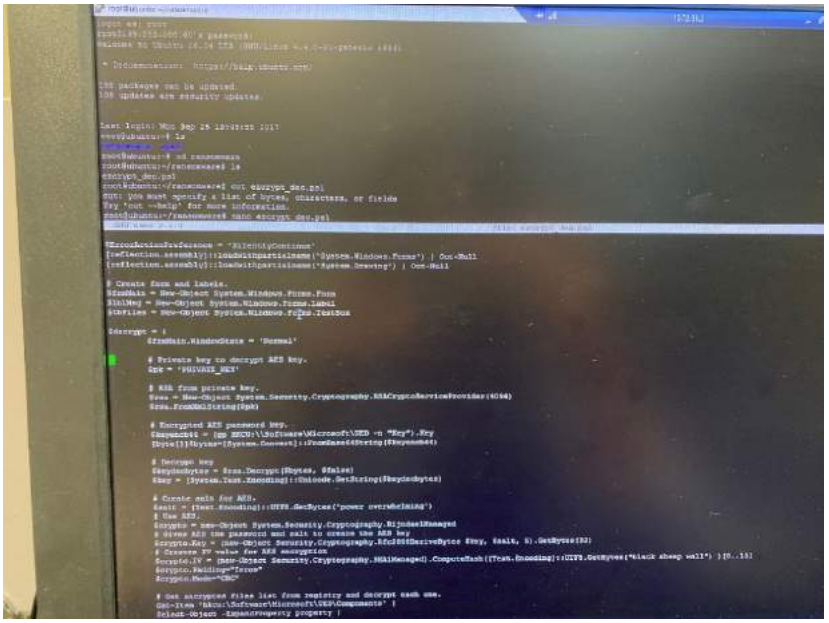


ראינו שהקבצים מוצפנים עם RSA

זה אומר שכדי לפענח קבצים אנחנו צריכים אלגוריתם הצפנה ומפתח הפרתי שלו

זה אומר שהדרך היחידה להחזיר את התוכן של קבצים מוצפנים היא לקבל את המפתח הפרטי של התוקף

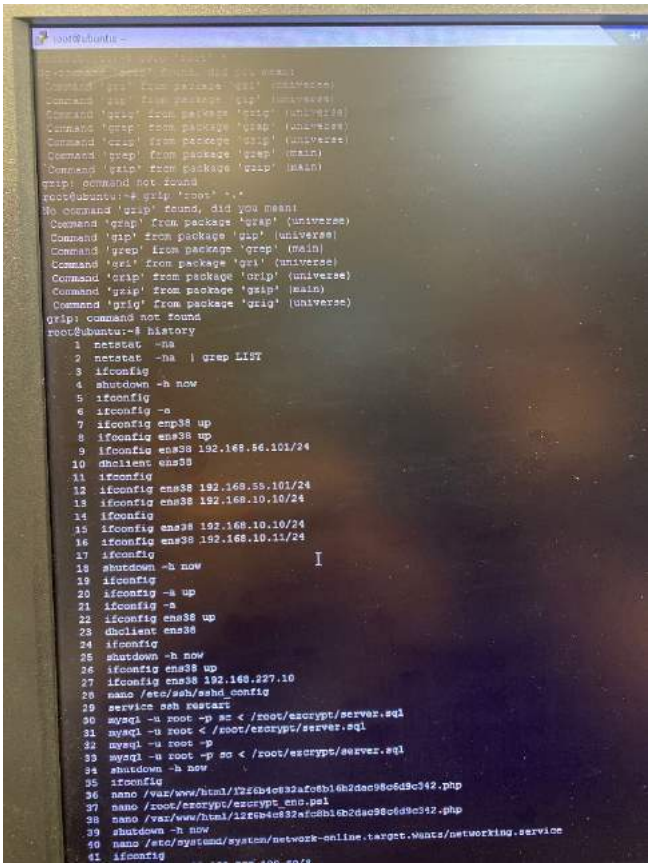
דרך putti נכנסנו למחשב של התוקף



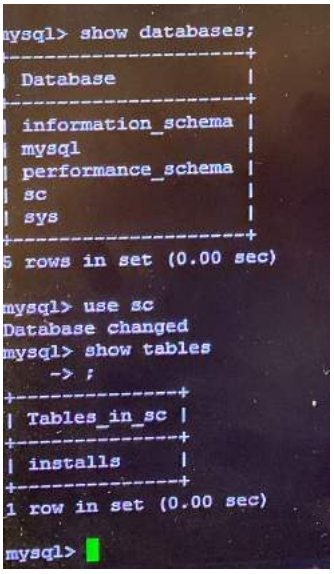
בעזרת ls מצאנו את תיקיית ransomware ונכנסנו אליה

בתסריט שלו, התוקף השתמש בשאילתות SQL, כלומר יש לו SQL מותקן

הפעלנו את הפקודה history במחשב של התוקף ובפקודות האחרונות שהקלדנו ראינו שהוא יצר מסד נתונים בשם SC




נכנסנו למסד נתונים זה




ואז נכנסנו לטבלה של installs

החלטנו למצוא את ה-UUID שנכתב עדיין בעמוד הראשון במסד נתונים זה

```
mysql> DEscribe installs;
+-------------+----------------+------+-----+---------+----------------+
| Field       | Type           | Null | Key | Default | Extra          |
+-------------+----------------+------+-----+---------+----------------+
| id          | int(11)        | NO   | PRI | NULL    | auto_increment |
| name        | varchar(45)    | YES  | UNI | NULL    |                |
| uuid        | varchar(255)   | YES  | UNI | NULL    |                |
| key_private | varchar(2000)  | YES  |     | NULL    |                |
| key_public  | varchar(2000)  | YES  |     | NULL    |                |
+-------------+----------------+------+-----+---------+----------------+
5 rows in set (0.01 sec)

mysql> SELECT * FROM installs WHERE uuid='KCC63IMT0AB';
```

מצאנו את המפתח.

```
New Text Document.txt - Notepad
File  Edit  Format  View  Help
qONrW0Hhdq6H2WVfmNXSD15VRMnXick9+pYcyQ+i76V9UxmCLxv0+EYZtzJsBfHGUNOJHM4i4iQ2UU0/gbU85k3cL6MfSJp9j5g79Uxkq9Ii2X2eWjhhVDLCJBZKYTgHXXFY
</Modulus><Exponent>
AQAB</Exponent>
<P>1SBZTxOV0GqQRVB30BKxm4GYEA43TNeWAAF99HW6FxTDbz3JYHy7+KxYrNoP6/EeiLw+vXuhDbV1NKxJ5UPGqw==</P>
<Q>ytzjH74308WxHmr+q8q7Q8H6aAEZrGtccpw4P/R8oViZQaFO1Wvy54M1F2OWpW+UxsCV3RIR0mJrxtcP60KMzQ==</Q>
<DP>e4pN2qWqs04khN1ZKja71z1uzNfAvH03SPeUcHERlrGFe+Uf5xtGxqX4nPGmSwkwvugHokSYnd6pNLgt+YSpEtw==</DP>
<DQ>GZCaos5y9KIuPvoW3AlxbgmNB/xTgvIItXzQbebeqejbazpZWX0N47EZt0r8/A23JE6kaCMQUJT+Lvzip9ZZQ==</DQ>
<InverseQ>amvdVZ/xeX0717T+Gp3o6ynZzo9X+J/y3NZ8cWwBbpYvHjyZPWJ7kfU859Nb6cYB1aV4mtZn0qAWaGe19vUboQ==</InverseQ>
<D>Zxezn9geTfkJ2g2EhmH3QGga+su083/RgpaBacZOuqS1VLWcfy88oRUBe4+e2x4T5aDK8LdwGcTrF0P1QUM1sZ31G2ZQ6X9R/ywTR9X4yNicub/UpBsjUD2bqGX0c915bwnCu9
</RSAKeyValue>
| <RSAKeyValue><Modulus>qONrW0Hhdq6H2WVfmNXSD15VRMnXick9+pYcyQ+i76V9UxmCLxv0+EYZtzJsBfHGUNOJHM4i4iQ2UU0/gbU85k3cL6MfSJp9j5g79Uxkq9Ii2X2eW
```

החלפנו בבתסריט את המפתח הציבורי שהיה לנו עם המפתח הפרטי הזה

```
$ErrorActionPreference = 'SilentlyContinue'
[reflection.assembly]::loadwithpartialname('System.Windows.Forms') | Out-Null
[reflection.assembly]::loadwithpartialname('System.Drawing') | Out-Null

# Create form and labels.
$frmMain = New-Object System.Windows.Forms.Form
$lblMsg = New-Object System.Windows.Forms.Label
$tbFiles = New-Object System.Windows.Forms.TextBox

$decrypt = {
        $frmMain.WindowState = 'Normal'


        # Private key to decrypt AES key.
        $pk = 'qONrW0Hhdq6H2WVfmNXSD15VRMnXick9+pYcyQ+i76V9UxmCLxv0+EYZtzJsBfHGUNOJHM4i4iQ2UU0/gbU85
```

הפעל את התסריט והחזיר את כל הקבצים

שיטות הגנה:

עדכן תוכניות ומערכת הפעלה בזמן

אל תאחסן מידע בעל ערך במחשב

לעולם אל תעקוב אחר קישורים לא בטוחים

אל תפתח קבצים מצורפים חשודים בהודעות דואר אלקטרוני