דו"ח מעבדה- תרחיש מס' 4

פרטים:

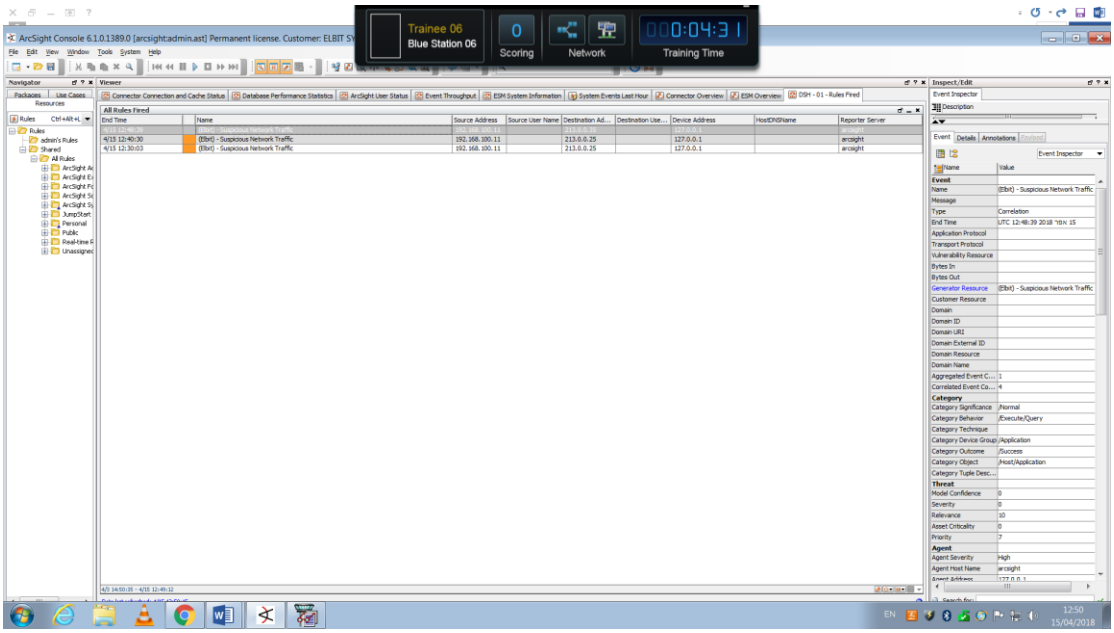
מגיש: שגיא סעדה

תאריך: 15/04/2018

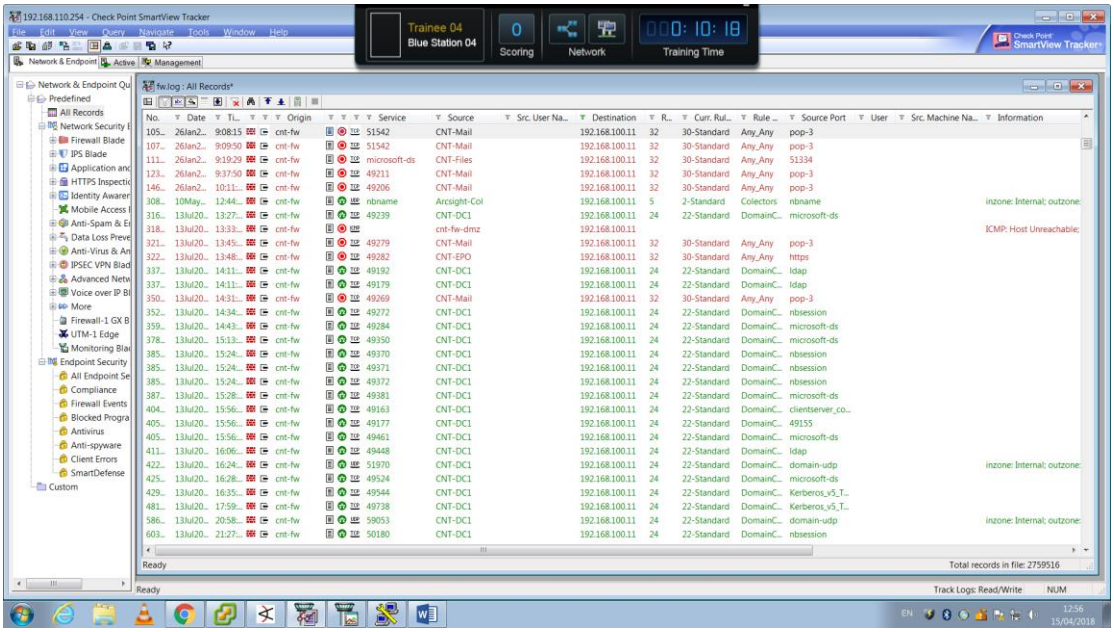
שם התרחיש: תקיפת עמדת עובד בארגון על ידי שליחת מייל עם קובץ זדוני.

תהליך ההתקפה:

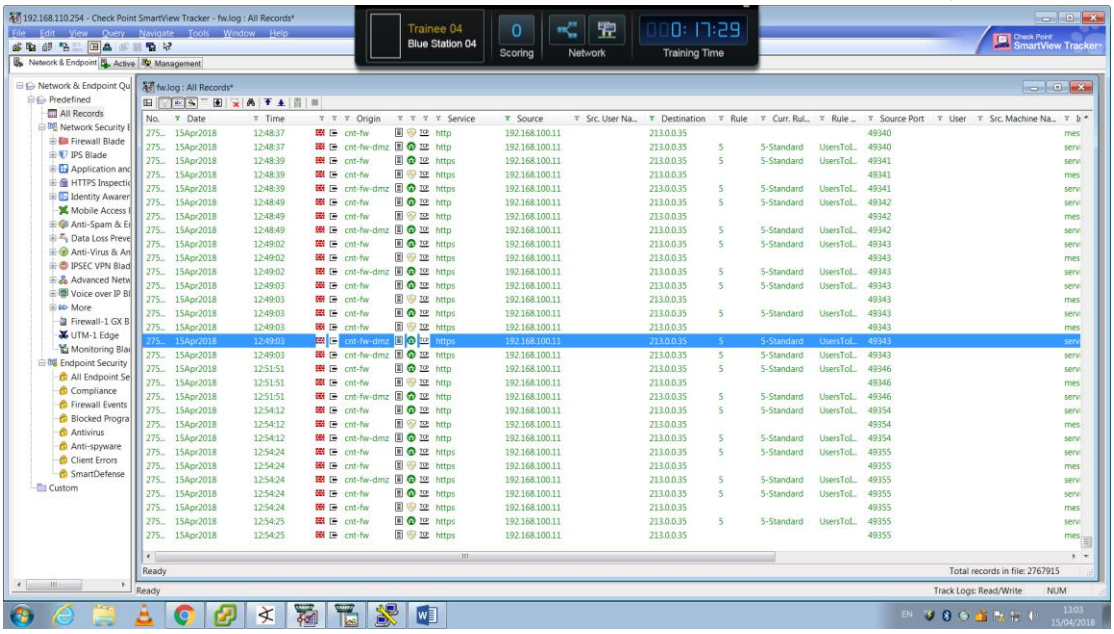
בתהליך ההתקפה זוהתה התראה על ידי הכלי ArcSight על תקשורת חשודה ברשת שלנו, מה- IP – 192.168.100.11 ל- IP- 213.0.0.35.



בנוסף, בכלי Tracker –

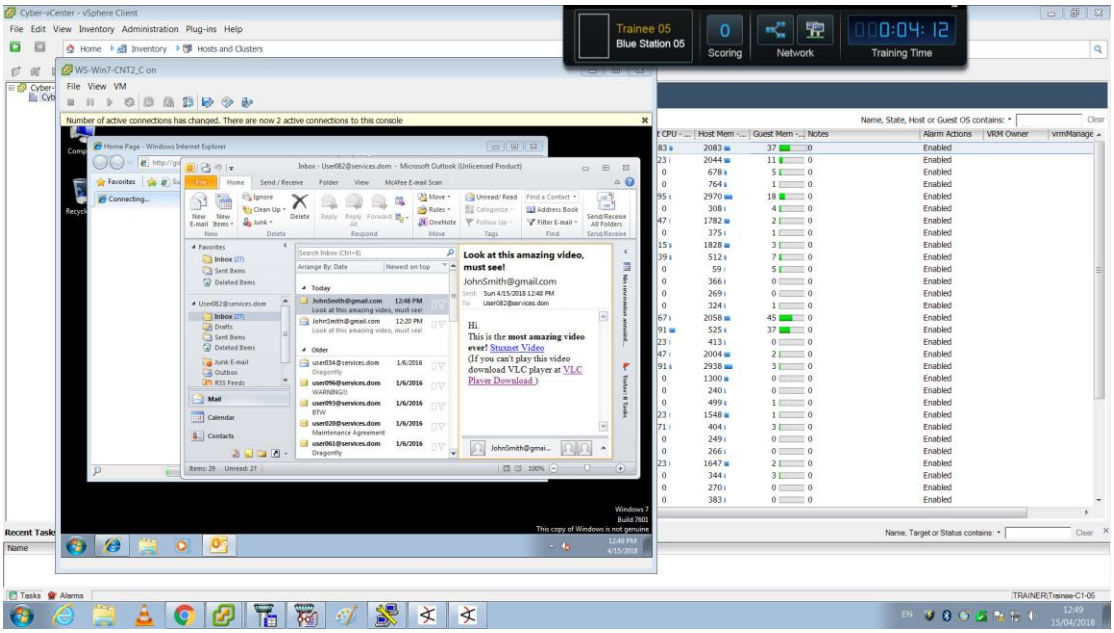


פעילות חשודה ככל הנראה, לאחר פילטור של כתובת היעד – 192.168.100.11.
תקשורת http ו- https בין ה- IP – 213.0.0.35 (IP שעדיין לא ידוע לנו) לבין – 192.168.100.11 (IP מהארגון).

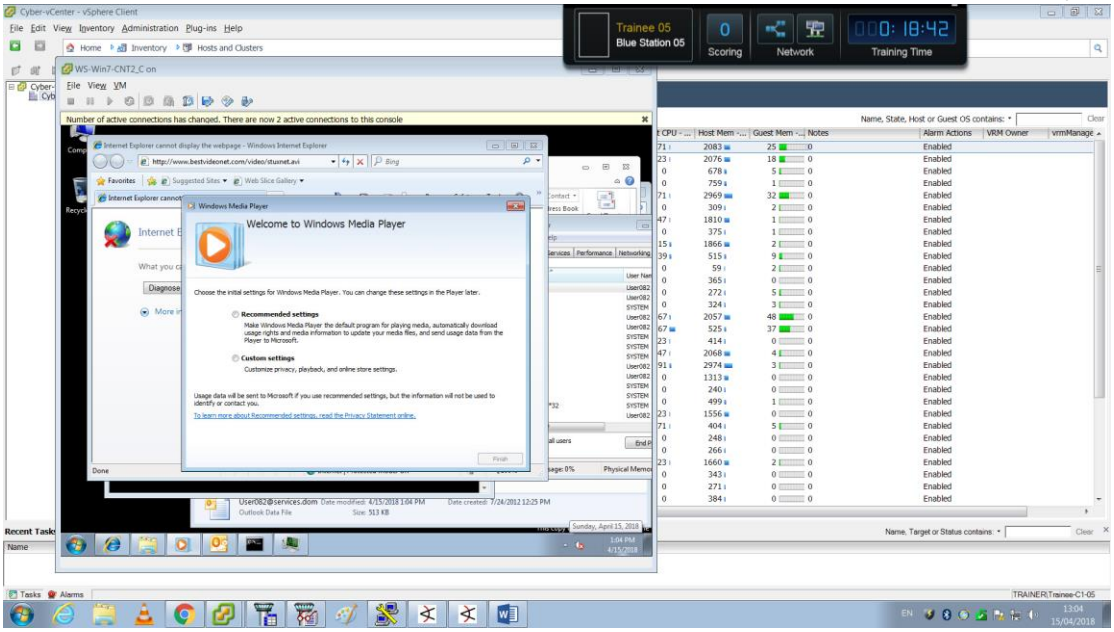


תהליך הזיהוי:

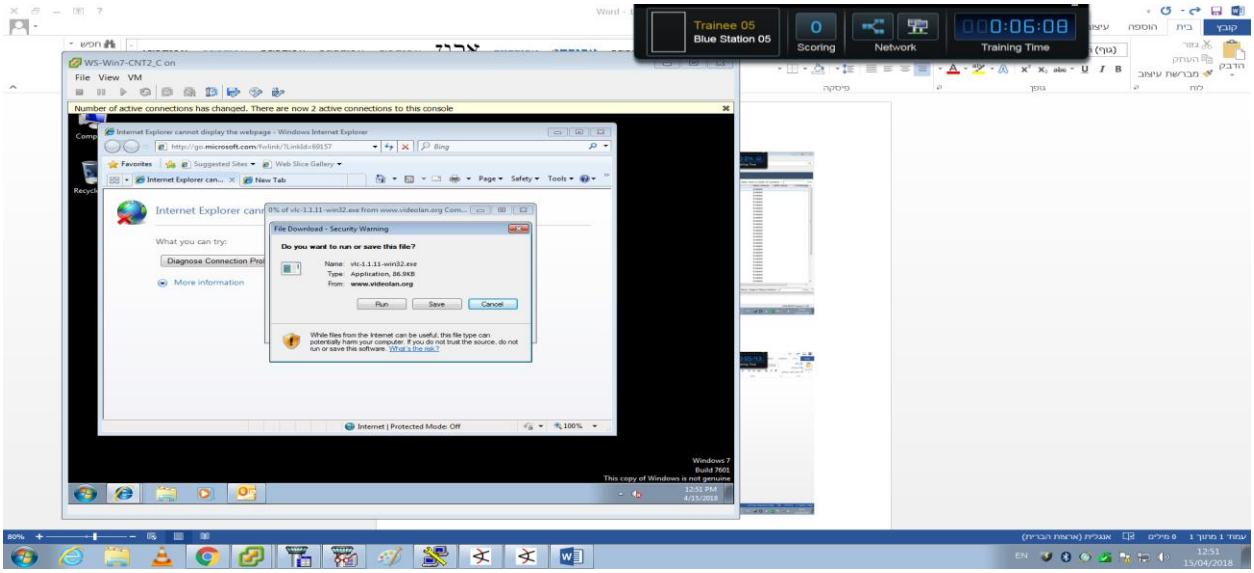
בתהליך הזיהוי ננקטו הצעדים הבאים על מנת להעמיק את הבדיקה של האירוע –
התחברנו לעמדה (עמדת עובד בארגון) והמסך שהיה פתוח הוא תיבת המייל, שם היה מייל שהתקבל לאחרונה –



ניתן לראות מייל שנקרא – Look at this amazing video, must see!
התקבל מ- JohnSmith@gmail.com
תוכן ההודעה – קישור לצפייה בסרטון והודעה שאם לא מצליחים לצפות יש להוריד VLC Player בעזרת הקישור המצורף.
לאחר מכן, ניסינו לגלוש לקישורים.
כשנכנסים לקישור הראשון של הסרטון עצמו, קופץ לנו חלון להתקנת Windows Media Player



בקישור השני לאחר שאנו לוחצים עליו להורדת VLC, כשאנו מריצים, לא קורה כלום.
מה שנפתח הוא קובץ הרצה (סיומת exe).



התחלנו לחקור את העמדה ולבדוק איפה מתקיימת התקשרות ל- IP החשוד.
הרצנו netstat וראינו שיש חיבור פעיל בין העמדה ל- IP החשוד (213.0.0.35) ב- https.
כמו כן היה חיבור נוסף סגור בין העמדה ל- IP הנ"ל באמצעות http.

<u>מסקנה -</u> קובץ ההורדה חשוד ולכן נרצה לחקור אותו.

בנוסף, נרצה להריץ WireShark על העמדה ולבדוק את התקשורת. (אך אין WireShark מותקן על העמדה).
ולכן, נשים לב שיש לנו שרת קבצים 192.168.200.6 בארגון שהוא מאפשר להתקין דרכו WiresShark או שניתן דרך <u>Sysinternals</u> לחקור כיוונים נוספים.

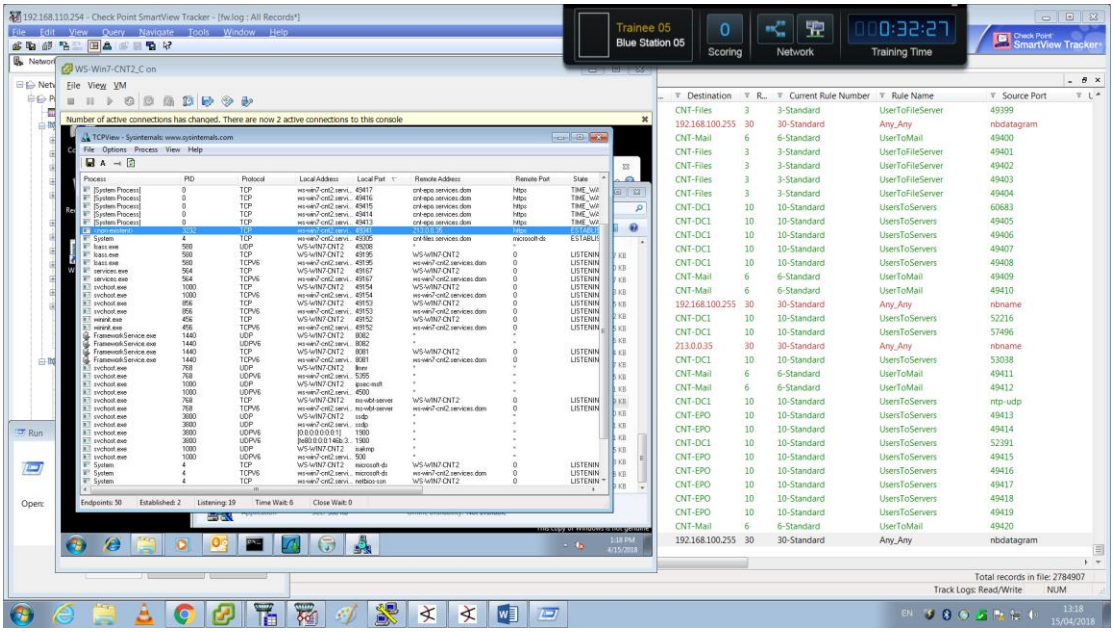
<u>Sysinternals</u> – הם אוסף כלים לניהול, אבחון, ניטור ופתרון בעיות בסביבת חלונות מבית מיקרוסופט.
האוסף מכיל כ- 72 כלים ופותח על ידי צוות המפתחים של חברת Winternals.
סוגי כלים –

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

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

ניגשנו לשרת דרך ה- run (כונן שיתוף) בהכנסת IP Address//

לאחר מכן, חיפשנו באינטרנט מה ב- Sysinternals יכול לעזור לנו לחקור קובץ בעמדה.
נכנסו לכלי TCPView וראינו את התקשורת בין העמדה ל- IP – 213.0.0.35.



בנוסף, ראינו שיש גם Process Monitor, אשר נותן מידע על כל Process, המקור שממנו הגיע ועוד.

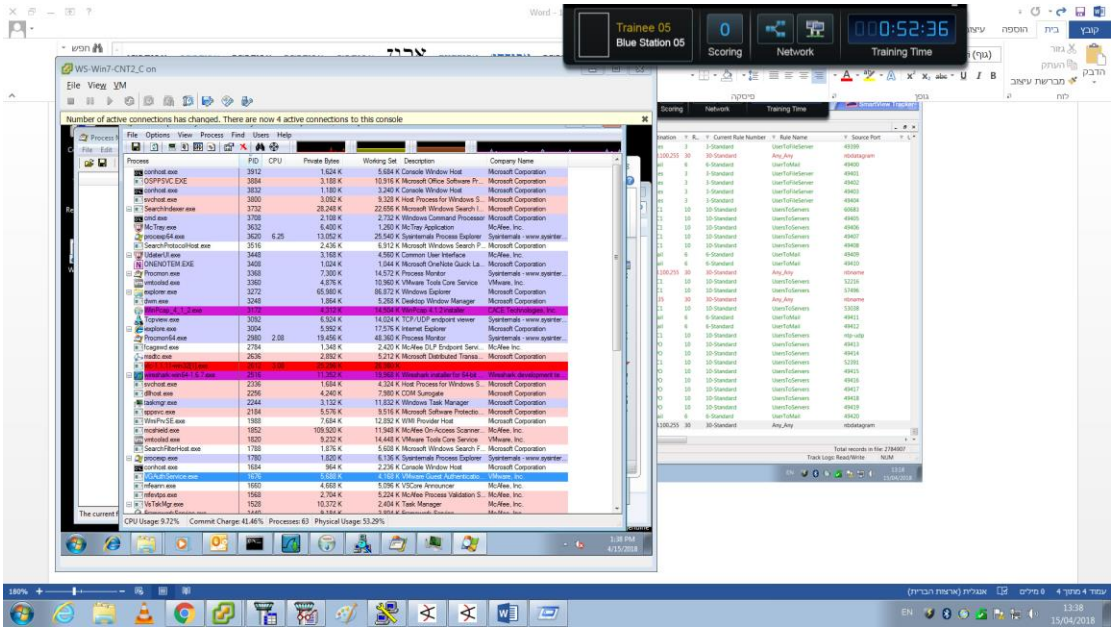
פתחנו את Procmon שככל הנראה הוא ה- Process Monitor.
ראינו דרך ה- TCPView שאין שם ל- Process של הקשר בין ה- IP החשוד לעמדה, אך כן יש PID.
חיפשנו לפי ה- PID – 3232 ב- Process Monitor.
לא מצאנו את ה- Process עצמו שם, כי טובעים בנתונים והחיפוש אינו יעיל.
הרצנו netstat -b על מנת לבדוק מה ה- PID שמקושר, לוודא שהוא באמת 3232 אבל מה שיקבלנו הוא system.
את ה- PID של הקובץ אנחנו רוצים למצוא, בדרך כלל ה- Process שנפתח מרצת קובץ הוא בשם דומה לשם הקובץ המורץ.
אם כך, כנראה שה- PID 3232 שהסתכלנו עליו הוא ה- PID של התקשורת ל- IP – 213.0.0.35.

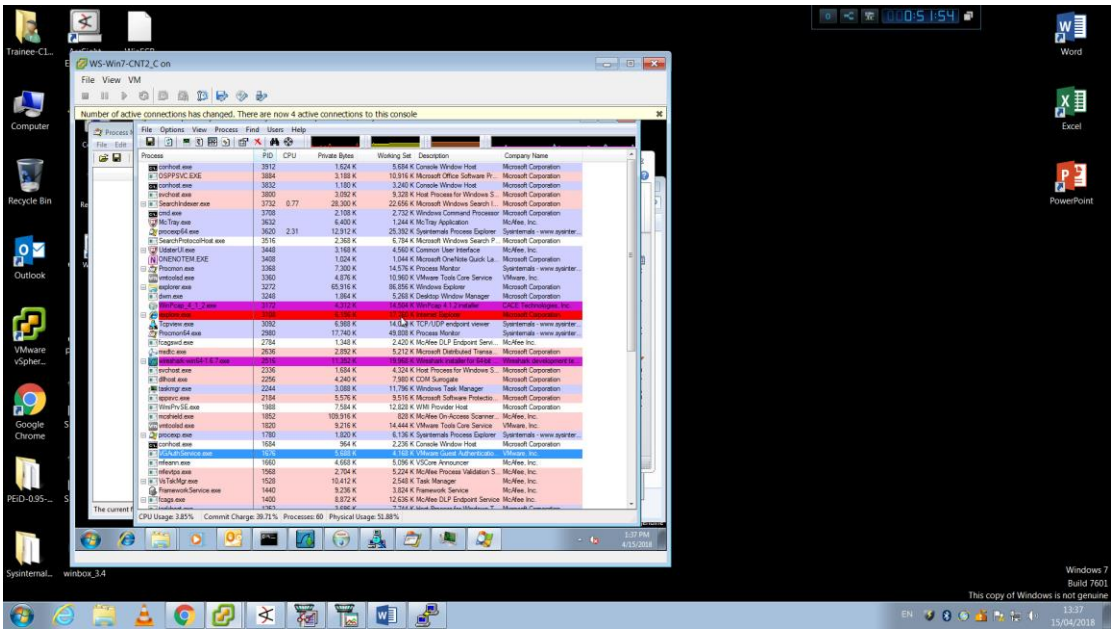
<u>בעיקרון מה שעושים בטיפול בהתקפות מסוג זה עם הקבצים הנלווים –</u>

הרצה של הקבצים בסביבה מוגנת, לא מריצים על המחשב בתוך הרשת שלנו כי מן הסתם יכולות להיות לזה השלכות.
בתרחישים אנו עושים זאת כי זה לא מציאותי להעביר את הקבצים לסביבות שונות ולבזבז על זה זמן.

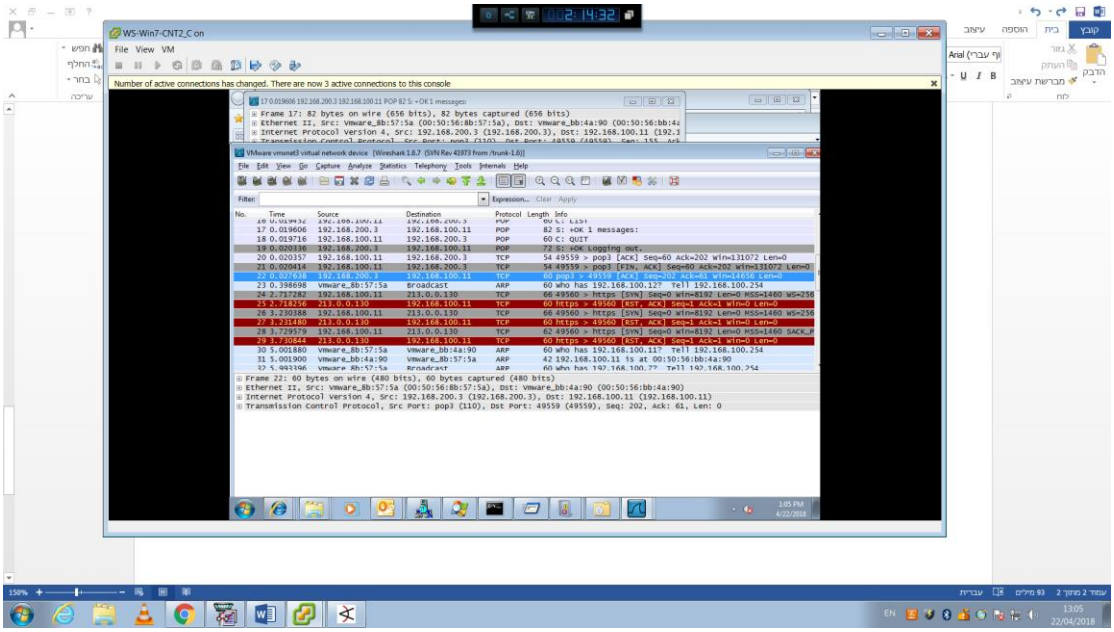
דרך ה- Process Monitor לא הצלחנו להשיג את מה שאנו רוצים אז המשכנו לחפש ב Process Explorer.

בתוך ה- Process Explorer מכיוון שזה Real-Time, הרצנו את הקובץ של ה- VLC ואז ראינו שקופצת שורה הקשורה אליו עם VLC – Process Name בחלון של ה- Process Explorer.



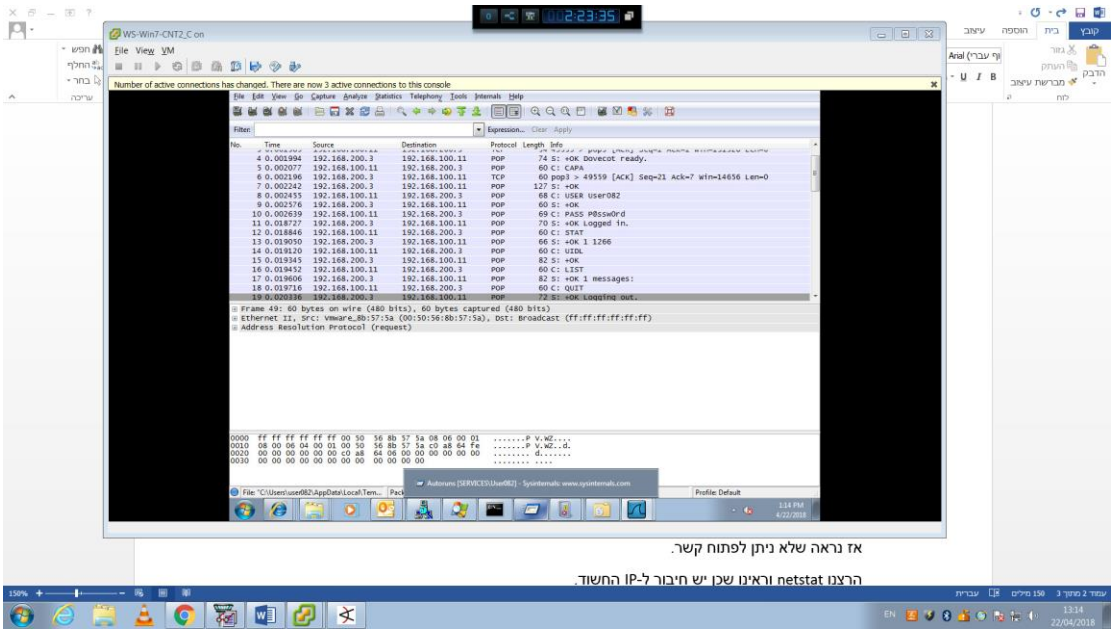


כעת, נבדוק דרך WireShark –
פתחנו WireShark והרצנו את הקובץ החשוד –



כאן רואים את הניסיון לפתיחת קשר שלנו לתוקף.

בנוסף, רואים את פרטי ההתחברות למייל של המשתמש, אבל זה גלוי בגלל שפרוטוקול POP3 בפורט 110 אינו מוצפן –



כמו כן, קיימים אתרים לבדיקה האם קבצים הם מוכרים כזדוניים.

הקלדנו את שמות הקבצים לתוך אתר Virustotal אבל אף אחד מהם לא העלה תוצאות רלוונטיות לתרחיש (מן הסתם Stuxnet העלה מיליון תוצאות אך לא מתאימות לקובץ שחיפשנו).

בשלב זה, עצרנו לחשוב - מדוע הקובץ שהרצנו נעלם אחרי כמה שניות בודדות ולמה אנחנו רוצים לפתוח קשר עם התוקף?

והגענו למסקנה שיש ניסיון לביצוע Reverse Shell.

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.

מה עומד מאחורי הרעיון הזה? מפני שקשה יותר לגרום לכך שהתוקף יצור קשר עם הנתקף מכיוון שהנתקף יושב מאחורי NAT והתוקף אינו יודע את ה-IP המקורי של הנתקף וכך ניתוב השיחה אל הנתקף יהיה בעייתי. תקיפה זו נקראת Bind Shell.

Bind Shell – לינק להמחשה - https://www.youtube.com/watch?v=M4oOgRWNIoE

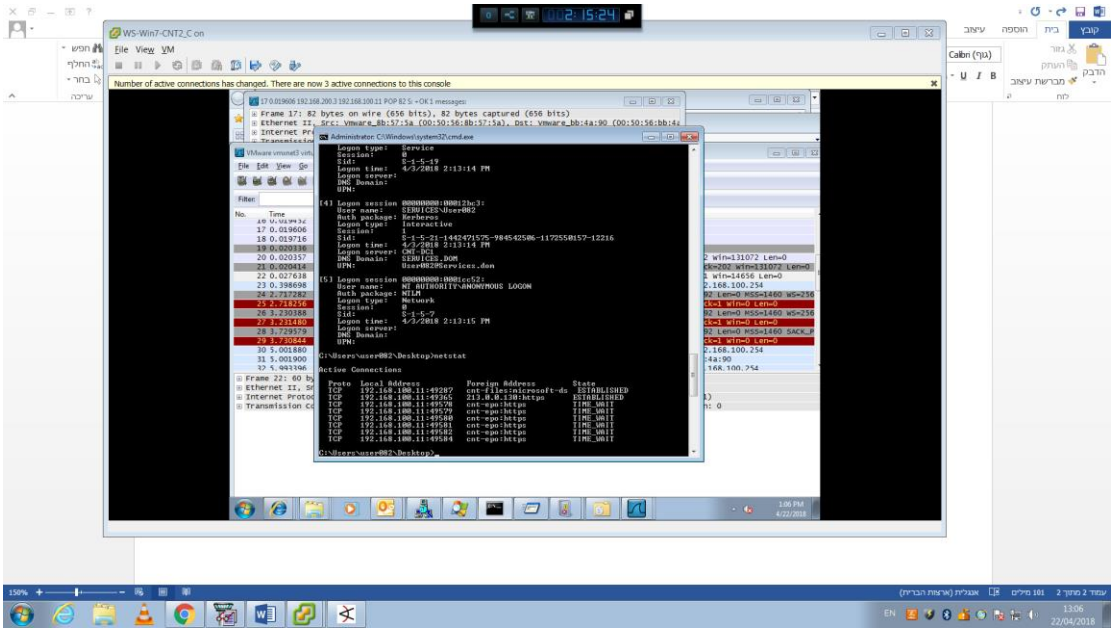
לדוגמא, רשת מחשבים שיושבת אחרי NAT שדואג לכך שה- IP החיצוני יהיה שונה מה- IP הפנימי של המחשבים. התוקף הכניס קוד זדוני לאחד המחשבים וגרם לו להאזין לפורט 4444 למשל. לאחר מכן, התוקף מנסה ליצור קשר עם אותו מחשב ספציפי אך תהיה לו בעיה, הוא יפנה ל- IP החיצוני של אותה רשת מחשבים ולא יצליח בקלות להגיע למחשב הנתקף ולכן, Reverse Shell הוא פתרון מצוין.

נחזור למקרה שלנו, מדוע בוצע Reverse Shell? והאם הוא נכשל? התשובה היא כן.

מכיוון שראינו שכאשר אנו מריצים את קובץ הזדוני שהורדנו דרך הדואר האלקטרוני של העמדה הוא ישר נופל ולכן המסקנה היא שהניסיון כשל.

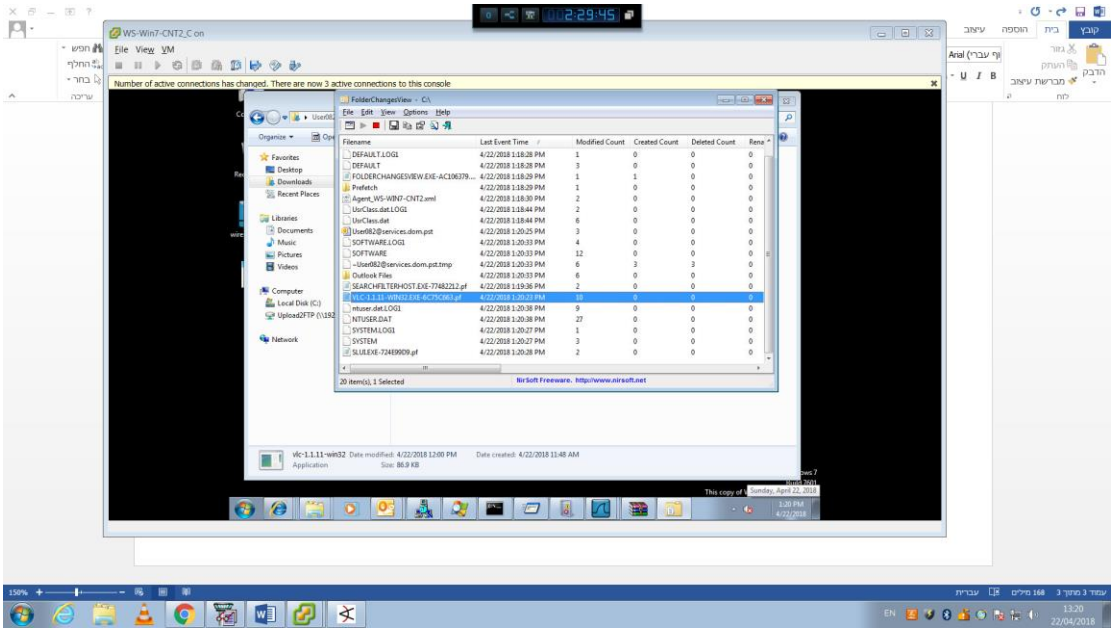
אז מה בדיוק התוקף עושה? מכיוון שהתוקף כבר הצליח להתחבר אלינו, פעולת ה- Reverse Shell נכשלה.

ניתן לראות הוכחה לכך שהתוקף מחובר אלינו דרך netstat –



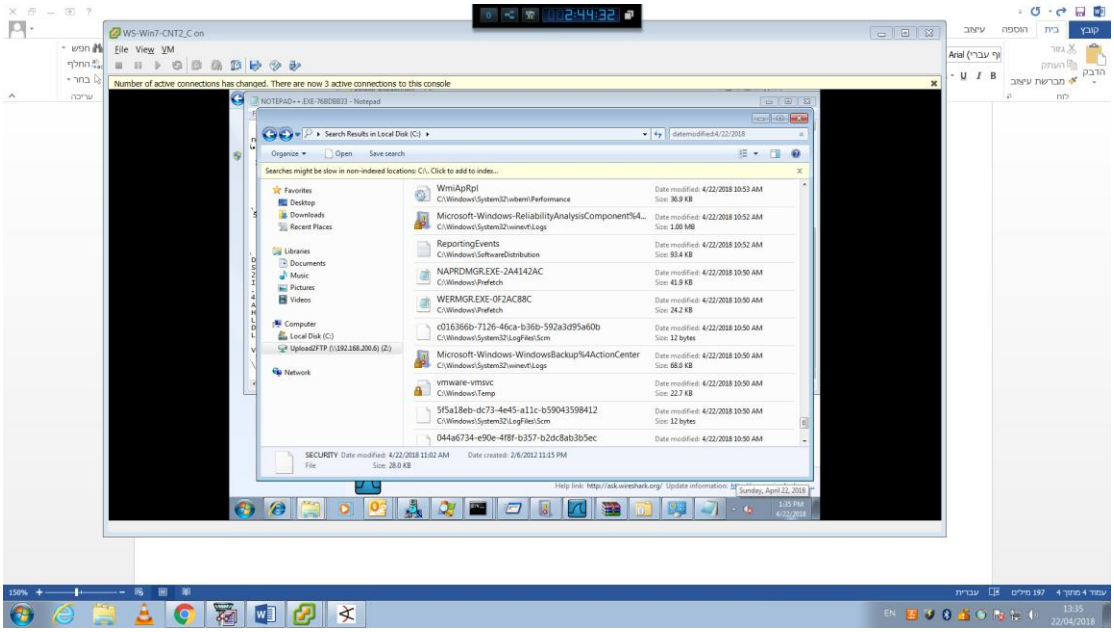
בשלב זה, כאשר אנו יודעים מה הקובץ עצמו עושה, נפסיק לחקור אותו ונעבור לשינויים שקרו בעקבות התקיפה.

באמצעות הכלי FolderChangesView ניתן לראות שינויים שקורים בזמן אמת בתיקיות ובקבצים במערכת.



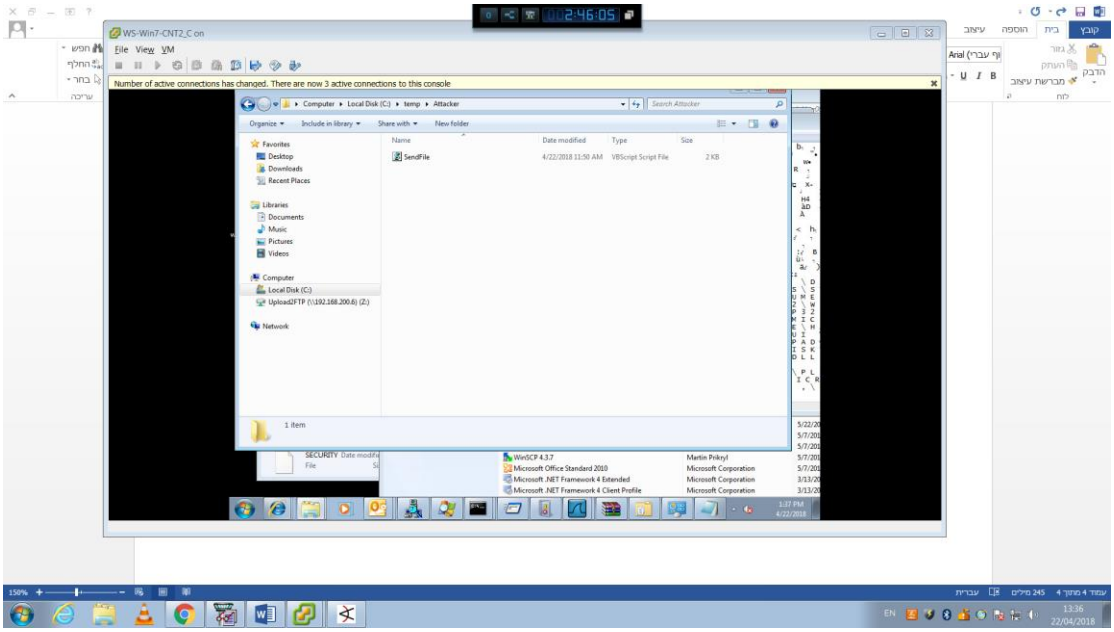
הכלי FolderChangesView לא עוזר לנו כיוון שהקובץ כמו שהבנו לא באמת מצליח לרוץ ולכן התקיפה כבר נעשתה בהתחלה.

חיפוש קבצים שהשתנו בדרך אחרת –

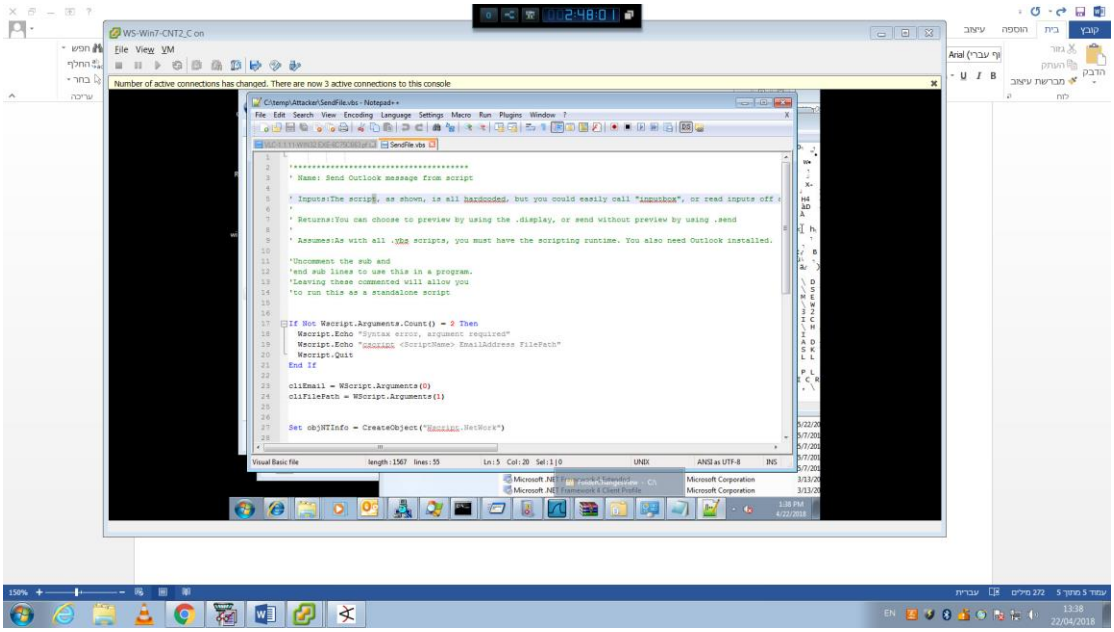


גם כאן זה לא כלכך צלח מכיוון שיש המון קבצים לבדוק.

באמצעות רמז, ניגשנו לתיקיית temp האהובה על האקרים ושם ראינו תיקייה בשם Attacker ובתוכו קובץ SendFile מסוג VBScript



תוכן הקובץ –



<u>הקובץ SendFile.vbs –</u>

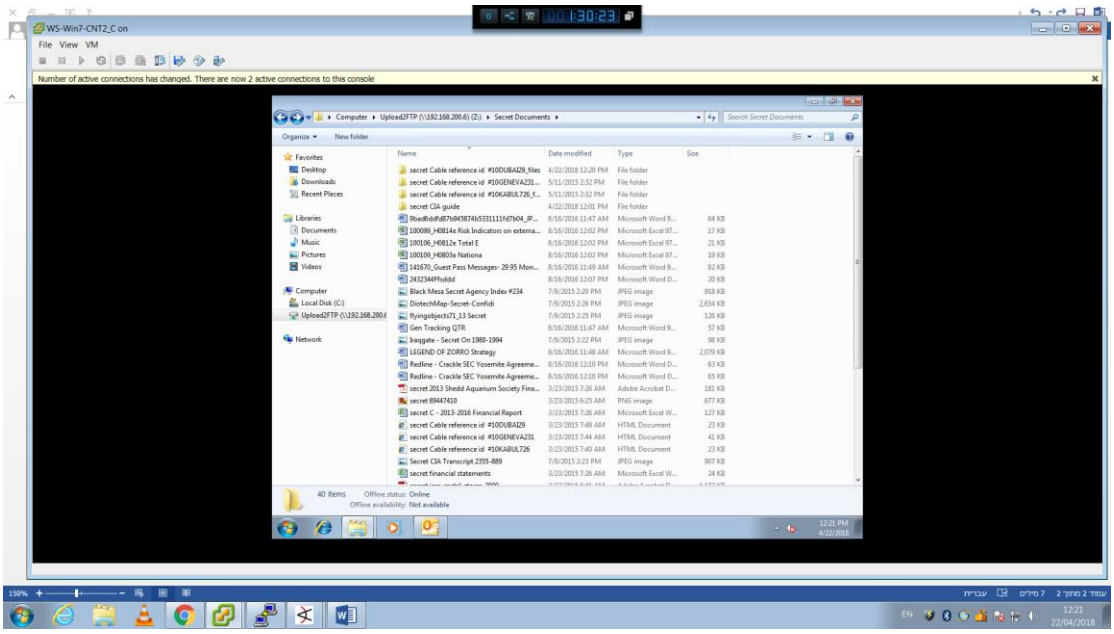
מאפשר למלא ולשלוח הודעת Outlook מתוך סקריפט.
כפי שניתן לראות בקוד – אלו הפקודות האפשריות
1 – פתיחת מייל
2- יצירת הודעה חדשה
3- הוספת קובץ מצורף
4 – שליחה
5 – ניקוי

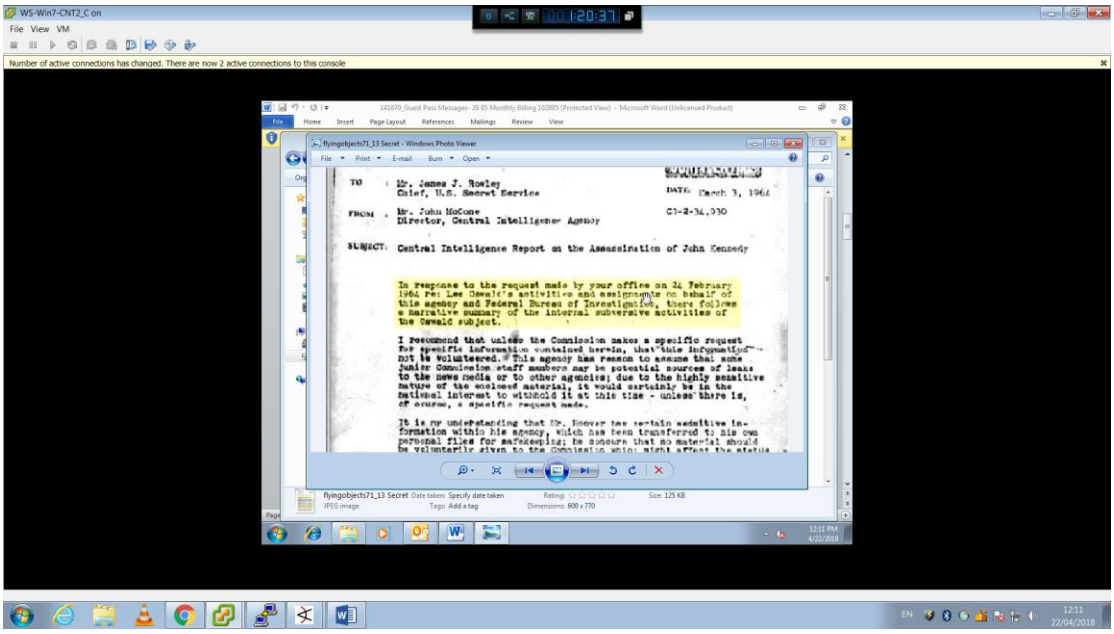
<u>VBScript –</u>

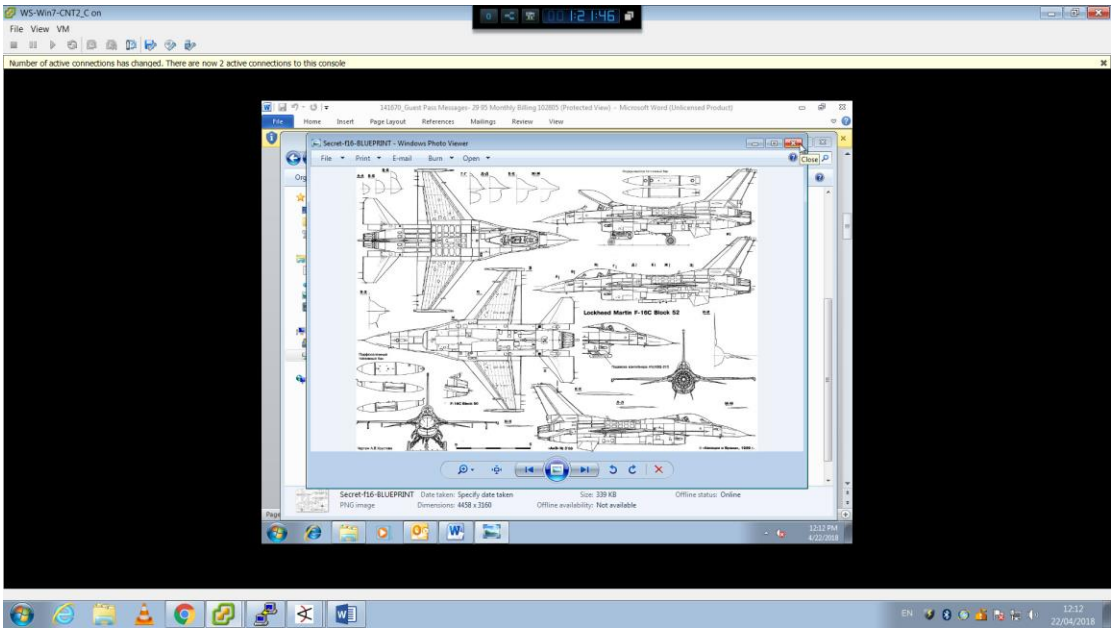
שפת תכנות מבית מיקרוסופט.
זוהי שפת Script בעלת תחביר המבוסס על זה של שפת Visual Basic, ואחת הכוונות בעת תכנונה הייתה שכל קוד VBScript תקין יהיה גם קוד Visual Basic תקין.
השפה משתמש בעיקר בסביבת מיקרוסופט השונות.
מקור - https://he.wikipedia.org/wiki/VBScript

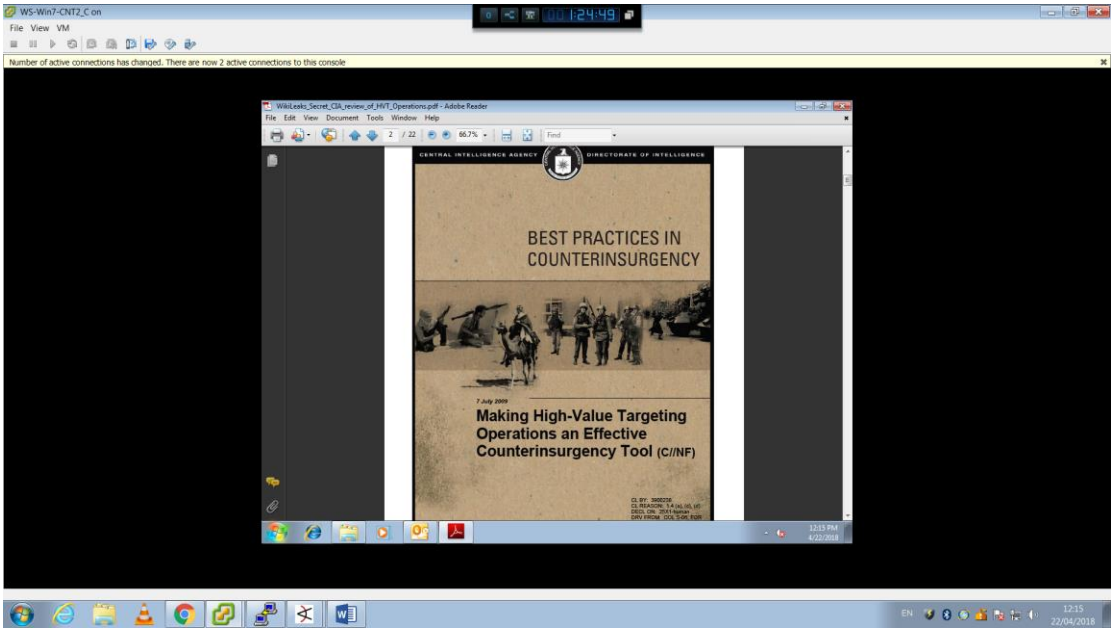
- אציין שבמהלך חקירת העמדה מצאנו מסמכים סודיים שקיימים בארגון –

כאשר נכנסים לחיפוש וכותבים 192.168.200.6// נפתחת תיקייה בשם Upload2FTP ושם נמצאים הקבצים הבאים –









מכאן, ניתן להסיק שהתוקף החדיר לעמדת העובד קובץ זדוני (SendFile.vbs) אשר שולח לתוקף באופן אוטומטי (Script) קבצים מתוך העמדה של העובד – ומפני שהעמדה מחוברת לשרת קבצים אירגוני, גם לשם יש גישה לתוקף.

תהליך הגנה:

בתהליך ההגנה, הבנו שאכן עמדת העובד היא העמדה המותקפת באמצעות זיהוי של הקובץ הזדוני וחיבור של התוקף ישירות לעמדה זו.

לכן, נצטרך למחוק את הקובץ ולנתק תקשורת עם התוקף.

תהליך הגנה מונעת:

בתהליך זה יש כמה דברים שכדאי לעשות בארגון כי למנוע תקיפה כזו –

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, Intezer – מערכת המאפשרת נראות של כל התוכנות והקבצים הפועלים בארגון.

בנוסף, יודעת לזהות באמצעות בדיקת DNA של הקובץ האם הוא קובץ זדוני או קובץ תקין.

ניתן לקרוא עוד על Intezer כאן - https://www.intezer.com/)

3 – מערכת הגנה עבור דוא"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.

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 נקודתית לעמדת העובד אשר משתמש במערכת ההפעלה Windows 7 ולכן האפשרות היחידה להתחבר הייתה רק דרך vSphere (רק סטודנט אחד יכול לשלוט על המערכת – מה שהתברר לבסוף שלא נכון - ניתן לשלוט על המערכת מכמה מחשבים בו זמנית).

מכאן, תוך חיפוש בעמדת העובד שאר הסטודנטים חקרו ברשת על תקיפות מסוג זה ו/או צפו בתהליך הזיהוי והמליצו על פעולות מסוגים שונים.

חוסרים/קשיים

-