דוי"ח מעבדה- תרחיש מס' 03

פרטים:

מגיש: אוראל מרדכי

תאריך: 05.12.18

שם התרחיש: WMI Worm

תהליך ההתקפה:

בשעה 14:00 קיבלנו התראה ב- ArcSight . בהתראה ראינו כי מבצעים על הרשת שלנו PingSweep, כלומר מיפוי של הרשת, זאת באמצעות שליחת ה- Pings ובהתאם לכך התוקף מצליח למפות את הרשת כולה ולדעת מי קיים ברשת ואיפה.

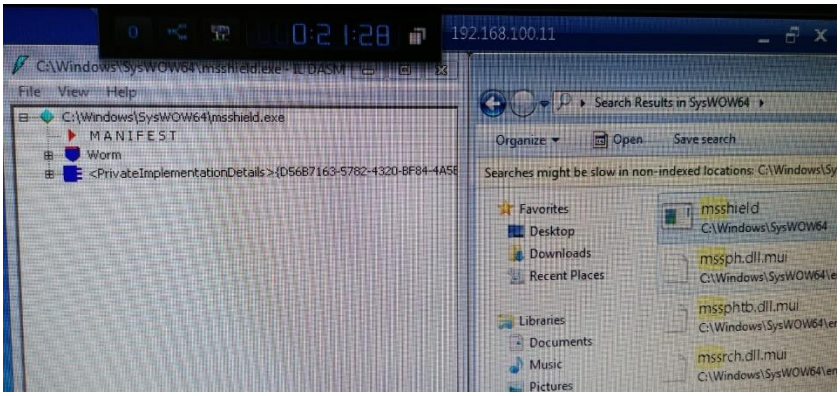
תהליך הזיהוי:

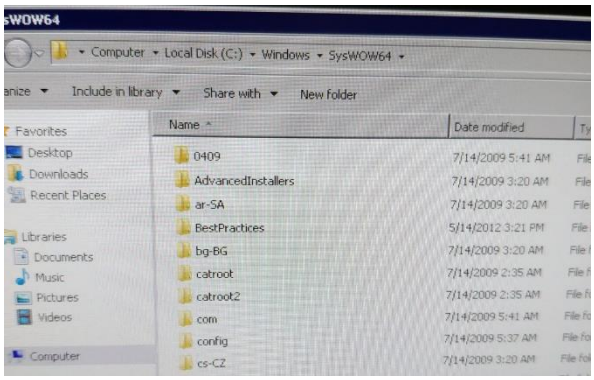
ניסינו תחילה לבדוק דרך ה ArcSight את כתובת התוקף ולנסות למצוא מאיפה מגיע ה- PingSweep. בהמשך אחרי חיפושים כי ראינו כמה כתובות מתוך הארגון שמבצעות PingSweep והחלטנו לבדוק את המחשבים בארגון באמצעות MSTSC על מנת לראות מה בדיוק קורה.

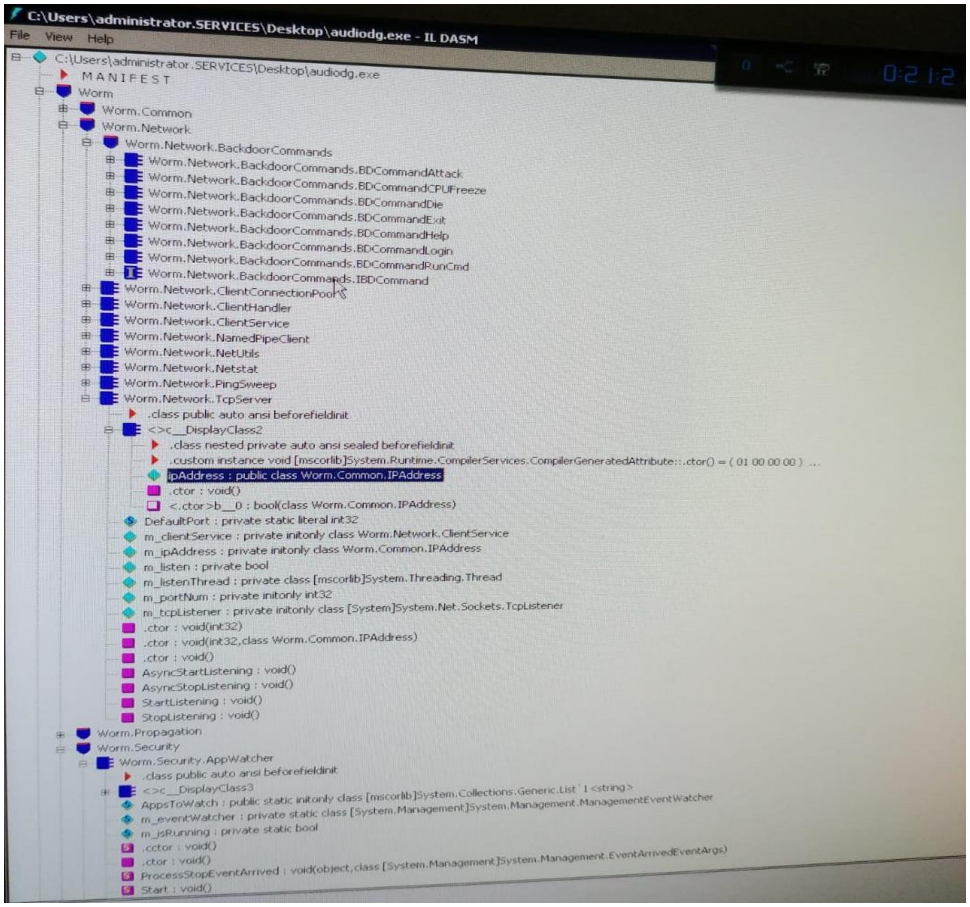
<u>תמונה להמחשה:</u>

לאחר בדיקה במחשב וחיפוש בתיקיות של המחשב גילינו בתוך תיקיית sys64WOW שתי קבצים חשודים שהתווספו בזמן שהתחיל התרחיש וזאת באמצעות ה -LAST MODIFY (הקבצים החשודים: msShiled.exe ו- winmy.exe). בשלב זה החלטנו לבדוק אותם. נעזרנו בתוכנה IL-DMSL זאת על מנת לבצע Reverse-Engineering לקבצים החשודים. גררנו את הקבצים לתוכנה ונוצר לנו Reverse-Engineering, והתוכנה זיהית לנו את הקבצים כתולעים.

תמונה להמחשה:



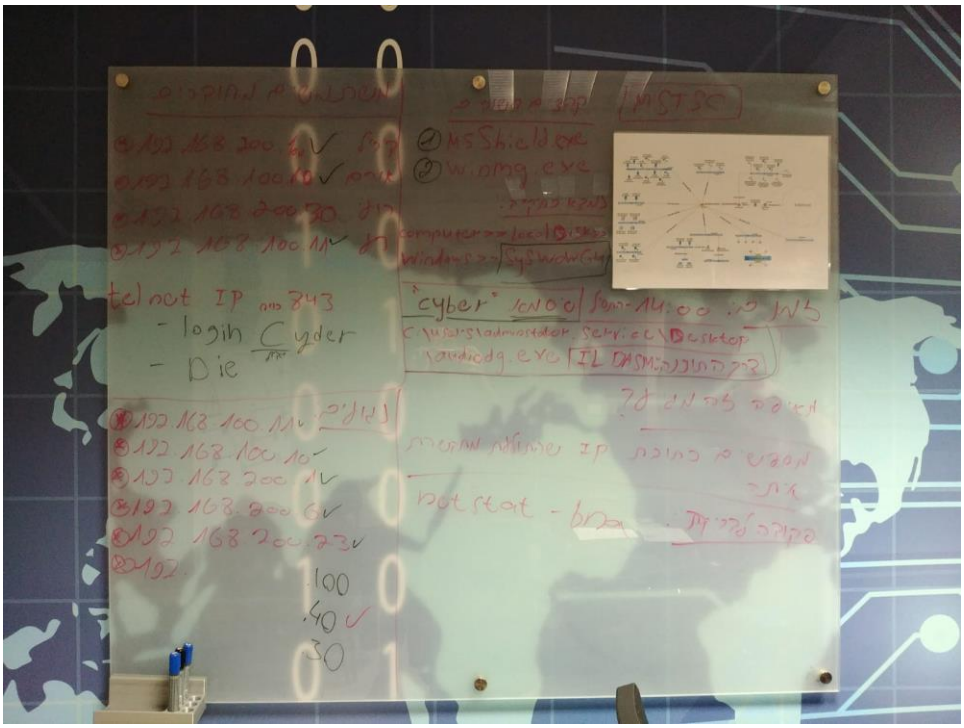




תהליך הגנה:

לאחר שזיהינו את הקבצים החשודים כתולעים ניסינו לשאול את עצמנו מאיפה זה מגיע. ביצענו בדיקה על כל המחשבים שבוצע דרכם PingSweep והתולעת התפשטה אולי ולסמן איזה מחשבים נגועים בתולעת.

תמונה להמחשה:

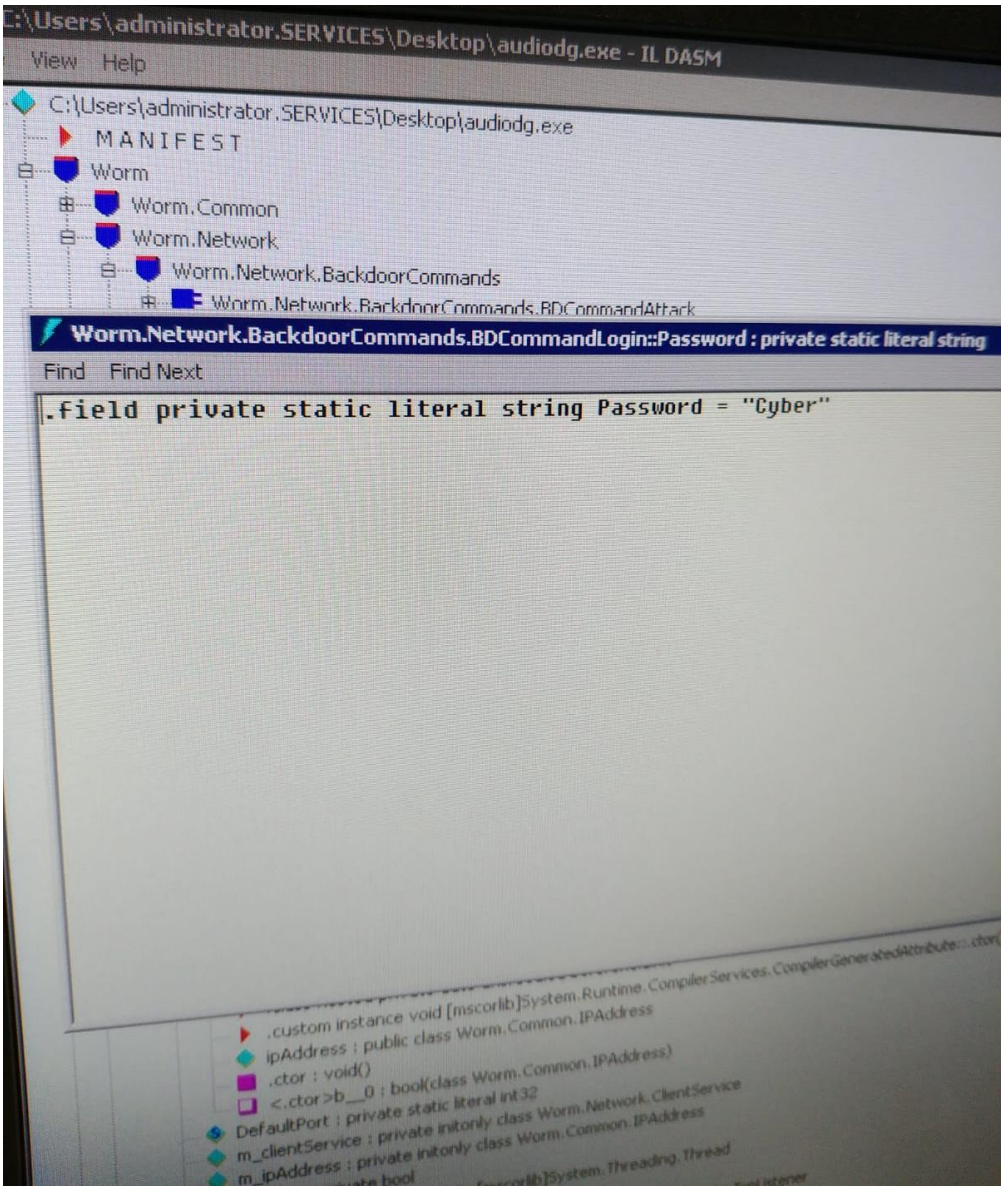


דרך נוספת שעזרה לנו לגלות איזה מחשבים נגועים היא באמצעות פתיחת מנהל המשימות ואם היה נתקע המנהל משימות היה אפשר לדעת בוודאות כי המחשב נגוע. ניסינו להעביר את המנהל משימות +לשנות את שמו אך לא כל כך הצליח לנו. בהמשך ניסינו לשאול את עצמנו מה בדיוק התולעת עושה והתחלנו לעלות השערות אם התולעת מוציאה מידע או מוחקת מידע.

תהליך הגנה מונעת:

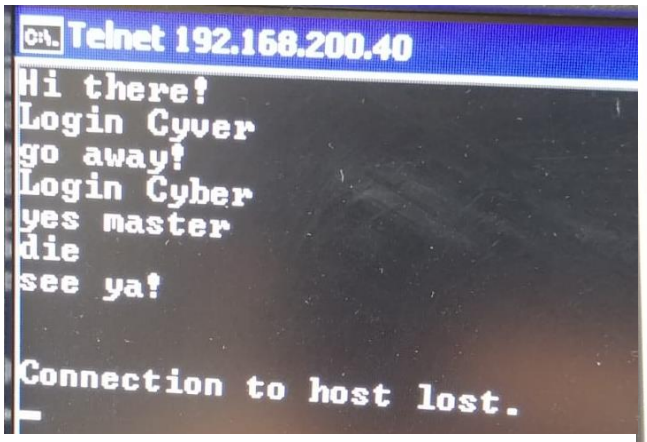
כאשר ניסינו להבין את השאלות מה התולעת עושה ומאיפה היא מגיע ניסינו לבדוק תחילה את דרכי התקשורת ולראות אם נוכל לזהות packets שנשלחות לאותו תוקף. באמצעות הפקודה netstat -bna הופיע לנו התוכנה(התולעת) וגם היה ניתן לראות לאיזה פורטים התולעת מדברת. גילינו כי התולעת מדברת לאחד המחשבים מתוך הארגון. אחרי בדיקה ראינו כי המחשב 192.168.100.10 הוא המחשב הראשון שהתריע ב- Arcsight בנוסף בדקנו אם לא נמחקו לנו קבצים במחשבים (לא נעשה מחיקה של קבצים). בהמשך התרחיש קיבלנו רמז לחפש על telnet ולאחר שבדקנו בגוגל ראינו כי זה חיבור לא מאובטח של ווינדוס ומפה כבר התחלנו להתקדם למציאת עצירת התולעת. לאחר מכן, באמצעות חיפוש בקבצי התולעת דרך התוכנה IL-DASM גילינו כי יש סיסמא שיכולה לעזור לנו אולי בפתיחת הקובץ לתולעת.

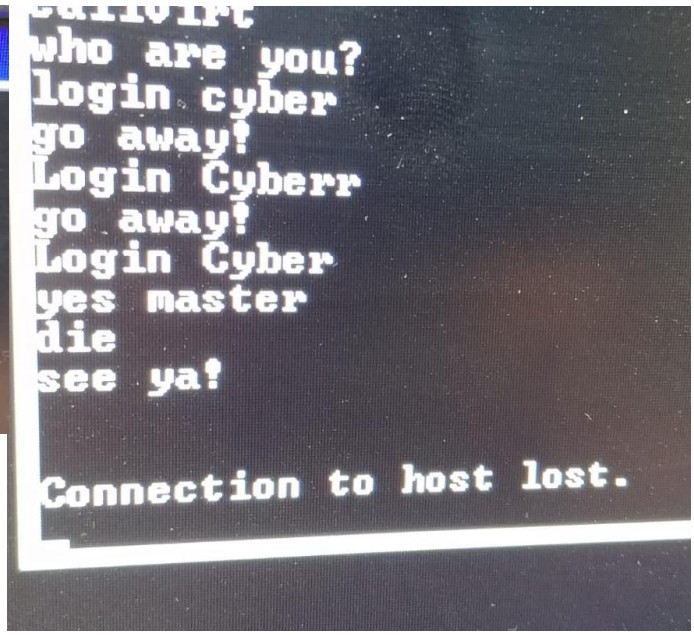
תמונה להמחשה:



בחיפוש באמצעות הtelnet גילינו ממשק שבו התוקף משתמש, בניסיון לדבר עם הממשק השתמשנו בסיסמא Cyber ולאחר מספר ניסיונות לא נתן שום דבר אז ניסינו דרכים אחרות עד שבסוף גילנו שכאשר אנו רושמים login cyber הממשק מנסה להרחיק אותנו אבל לאחר מספר ניסיונות של אותה הסיסמא הצלחנו להשבית את התולעת ולגרום לתוקף להתנתק.

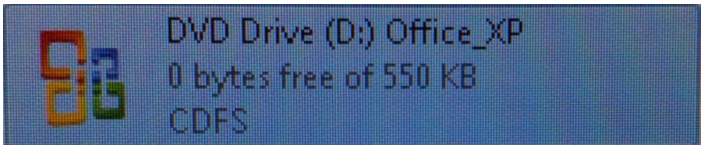
תמונות להמחשה:

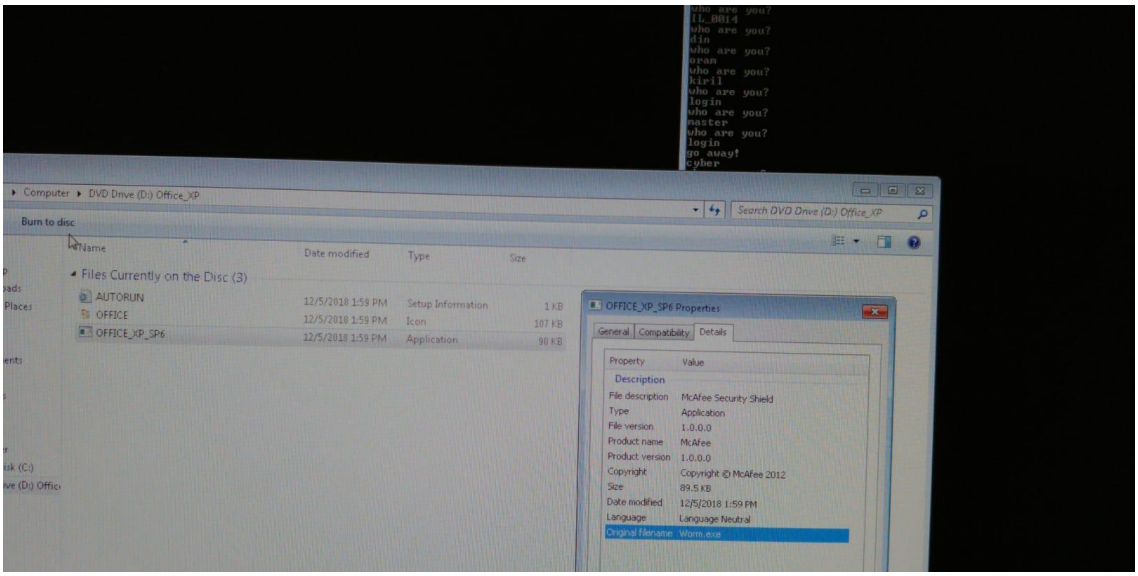


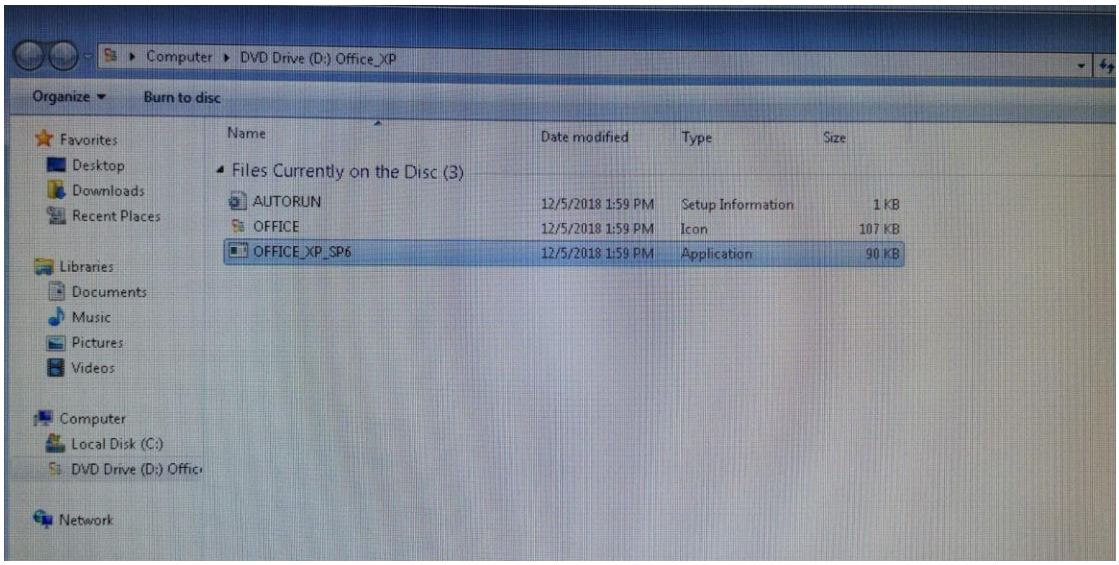


בשלב זה לאחר ששאלנו באיזה דרך הצליח התוקף להתחבר למחשב, העלנו את ההשערות כי יש USB שאחד העובדים הכניס למחשב או CD משהו חיצוני שהתחבר למחשב וראינו כי "במחשב זה" יש CD של אופיס שאחד העובדים הכניס למחשב. בבדיקה מהירה גילינו כי המקור לתולעת הגיע מה CD ובכך הצליח התוקף להתחבר למחשבים בארגון.

תמונות להמחשה:







הפרצות באבטחת הארגון

לא נעשה חסימה של המחשבים לקבלת התקנים חיצוניים כגון USB(דיסק און קיי), CD, ארד דיסק חיצוני וכו'... מה שגרם למחשבים להיות חשופים ופגיעים.

כלים שפיתחנו

אין

אופן עבודת הצוות

אוראל- ראש צוות

רועי- בדיקת מחשבים נגועים וחיפוש בגוגל

קיריל ואורם – מציאת פתרון והשבת התולעת

רע- בדיקת מחשבים נגועים ומעקב על המחשבים שבוצעו ה- PINGSWEEP .

ינאי- בדיקת מחשבים נגועים

חוסרים/קשיים

היה קצת קשה להבין בהתחלה מה אנחנו מחפשים ואיך לגשת לתרחיש הזה אבל בסה"כ הצלחנו להתמודד יפה כקבוצה.