

דו"ח מעבדה - תרחיש מס' 5

פרטים:

מגיש: דביר ברזילי

תאריך: 24.5.2018

שם התרחיש: WMI Worm

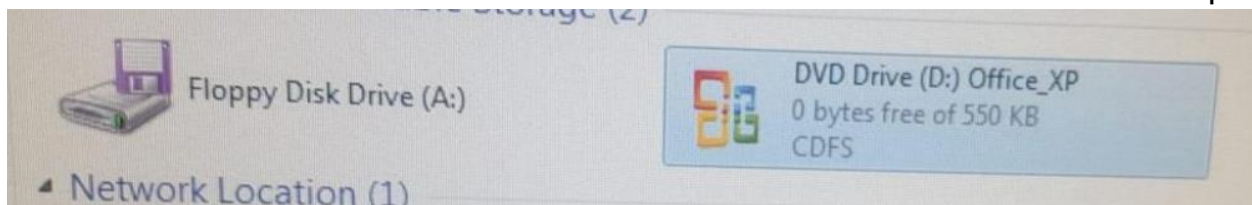
הסבר על בחירת שם התרחיש:

WMI או בשמו המלא Windows Management Instrumentation היא תשתית לניהול מידע ופעולות על מכוונות מבוססות Windows. באמצעות התשתית ניתן לבצע פעולות תחזוקה ולקבל מידע על מחשבים מרוחקים. באופן כללי ניתן לבצע כמעט כל דבר על מחשב מרוחק, כמו לדוגמא ביצוע התקנות על מחשבים בארגון, הסרה של התקנות, גיבויים או לחילופין לקבל מידע כגון מהם כל ה- Processes שרצים במערכת כרגע, איזו גרסה של Service Pack מותקנת, מתי מפעילים את ה-explorer ועוד מידע רב.

בתרחיש זה התולעת שהתפשטה במחשבי הארגון ניצלה את הכלי WMI ומנעה מהם לתפקד לאחר הרצה של אחד מהתוכניות שהתוקף קבע, וביניהם ה- task manager וה- process explorer. בדרך זו התוקף הקשה עלינו לזהות את אופי ההתקפה שלו והסווה את אופן השפעתו ושליטתו על המחשבים הנגועים.

תהליך ההתקפה:

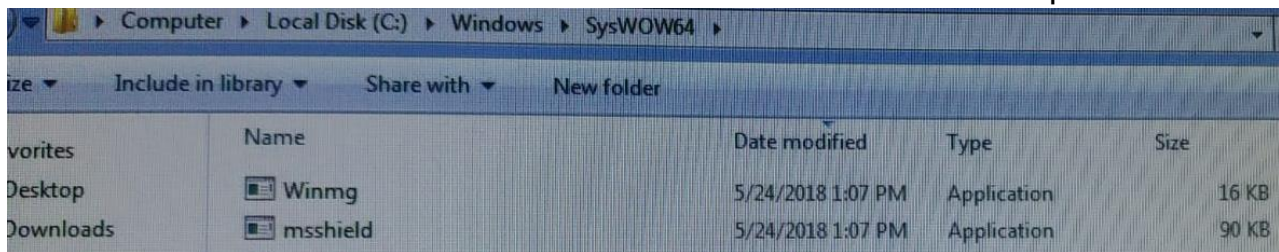
ההתקפה התחילה בעקבות דיסק של Office_XP שהוכנס לתחנת קצה והכיל בתוכו תולעת שהתפשטה ברשת של הארגון וגרמה לנזקים במחשבים רבים כמו פגיעה ביכולת המחשב להגיב כאשר מפעילים את התוכנה task manager. כמו כן התוקף פתח תקשורת עם המחשבים הנגועים ע"י שימוש בפורט 843 ושליחת פקודות לשליטה על המחשבים.



תהליך הזיהוי:

קיבלנו התראות על ping sweep detected ב-ArcSight והחלנו בחיפוש אחרי זברים חשודים שקרו במחשבים שעליהם התקבלה התראה. זיהנו שבכל המחשבים הללו יש התנהגות זרה – כאשר מפעילים את ה-task manager המחשבים מפסיקים להגיב. עשינו חיפוש מעמיק יותר בתחנה הראשונה שהתקבלה עליה התראה CNT-DC-1 וזיהנו שהוכנס אליה דיסק של Office_XP שמשקלו פחות ממגה (!).

בעזרת בדיקה אחר קבצים שהשתנו ברגע התקיפה מצאנו שתי תוכנות חדשות שהגיעו לכל אחד מהמחשבים הנגועים בשמות msshield ו-mgwing. עשינו לתוכנות הללו reverse engineering בעזרת ILDASM וגילינו שהם מכילות קודים זדוניים של נזקות רבות.



Computer > Local Disk (C:) > Windows > SysWOW64				
Size	Include in library	Share with	New folder	
Favorites	Name	Date modified	Type	Size
Desktop	Winmg	5/24/2018 1:07 PM	Application	16 KB
Downloads	msshield	5/24/2018 1:07 PM	Application	90 KB

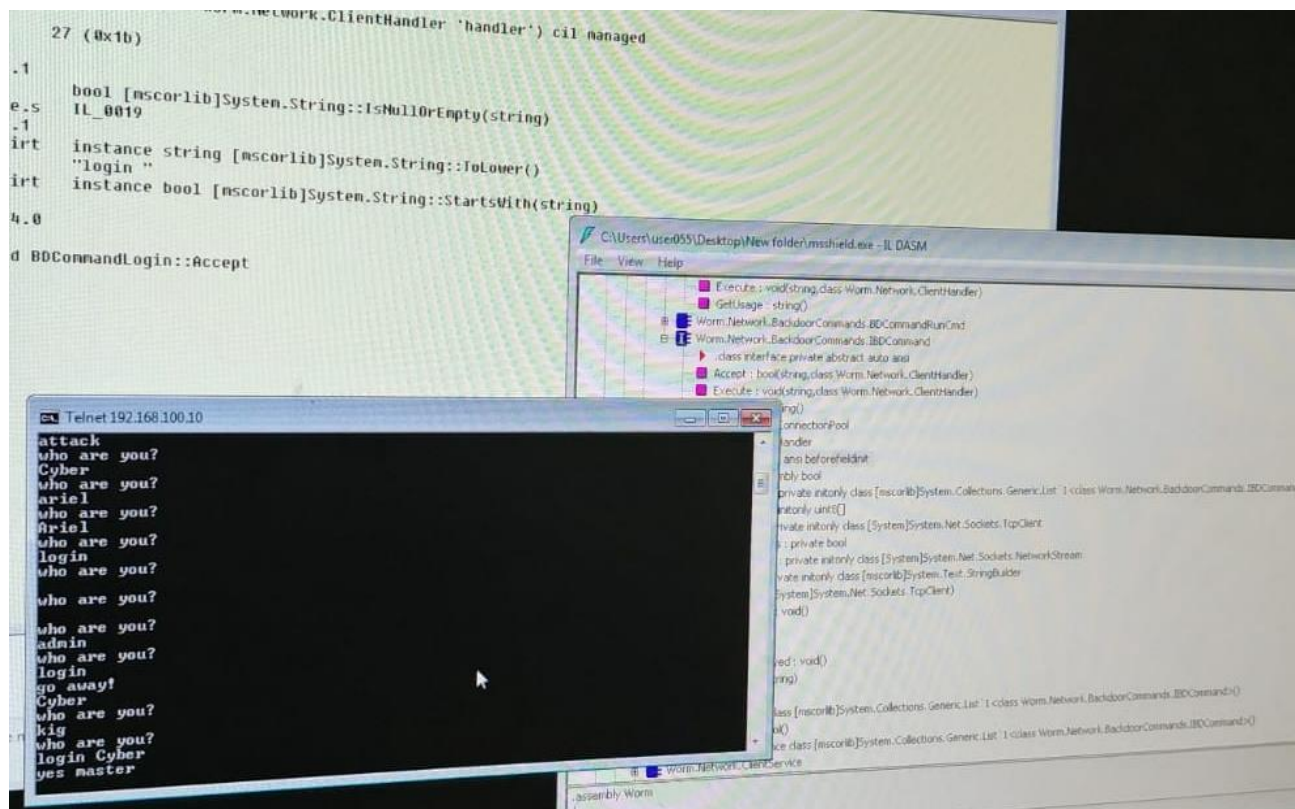
רצינו לבדוק מה מאפייני התהליכים שרצים על המחשב בעקבות הפעלת התוכנות הנ"ל ע"י שימוש בתוכנה Process Explorer אך גם בהרצת תוכנה זו המחשב הפסיק להגיב. מכיוון שהתנהגות זו של הנוזקה בהכרח תלויה בשם של התוכנה שאנו מעוניינים להריץ שינינו לתוכנה את השם ורק אז הצלחנו להריץ אותה.

בעזרת ה-Process Explorer יכולנו להבחין שהתהליך msshield יוצר תקשורת דרך פורט 843. על מנת לנסות להבין מה קורה כשהתוקף משתמש בפורט 843 כדי לתקשר עם המחשב המותקף ניסינו להתחקות אחריו ולהתחבר בעצמנו למחשב המותקף בפורט 843 ע"י שימוש ב-telnet.

```
Users\trainee-c1-05>telnet 192.168.100.10 843
```

כשהתחברנו התבקשנו לעבור תהליך הזדהות. מתוך העובדה שכל מחשב מותקף מצליח לאמת את שלב ההזדהות נובע שהנוזקה עצמה מכילה בתוכה את המפתח למעבר שלב ההזדהות ולכן חזרנו לתוכנה ILDASM (התוכנה שעושה reverse engineering) ומצאנו שם את ה-backdoor שבעזרתו מתבצע

תהליך ההזדהות (שם משתמש וסיסמה: login cyber). לאחר שהתוקף עובר את תהליך ההזדהות של ה-backdoor שארגן לעצמו הוא יכול להעביר פקודות למחשבים המותקפים ולשלוט עליהם.



תהליך הגנה:

ניקוי הנוזקה מהמחשבים הנגועים וסגירת פורט 843.

תהליך הגנה מונעת:

התקנת תוכנת אנטי וירוס על מחשבי הארגון. כמו כן אפשר לקבוע מדיניות שימוש בהתקנים מחמירה וכך להפחית את הסיכוי להחדרת נוזקה לתוך הרשת של הארגון.

הפרצות באבטחת הארגון

משתמשי תחנות הקצה מהווים מוקד לחדירה פשוטה לרשת של הארגון. ניתן להבחין שעד כה רוב התרחישים החלו מחדירה דרך תחנות הקצה.

אופן עבודת הצוות

מכיוון שהתולעת התפשטה על מחשבים רבים יכולנו לחקור כולנו יחד את מהלך התרחיש, כל אחד על מחשב נגוע אחר. שילבנו כוחות ושיתפנו ברעיונות והשערות על הדרכים שבהם התבצעה ההתקפה והדרך להתמודד איתה.

חוסרים/קשיים

התרחיש שאירע היה עשיר במורכבותו החל מאופן החדירה, אופן ההתפשטות במחשבי הארגון, השפעת הנוזקה על מחשבי הארגון ואופן השליטה של התוקף על המחשבים.