

דו"ח תרחיש-Worm WMI

1. לוגיסטיקה:

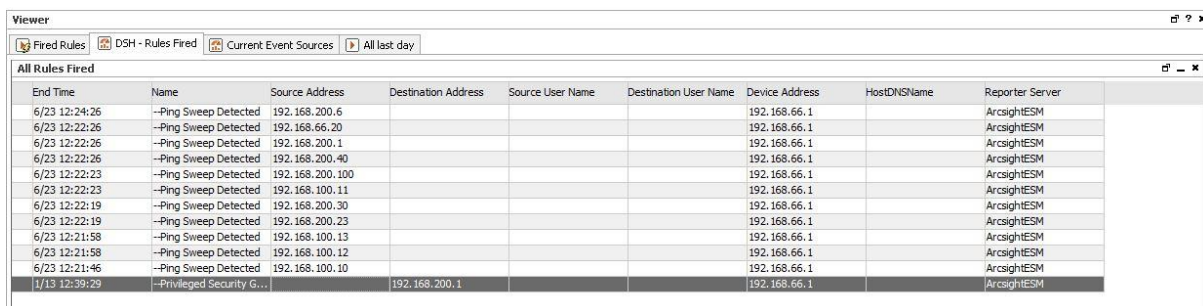
- A. שם מלא: אליהו פרידמן
 B. תעודת זהות: 211691159
 C. שם התרחיש: WMI Worm

2. תהליך זיהוי התקיפה:

בשלב הראשון, התקבלה התראה במערכת ARCSIGHT של Ping Sweep על 11 מכונות שונות בארגון, כולם עם מערכת הפעלה Windows.
 נשים לב כי המכונות הם משלושה אזורים שונים: User Segment Server Segment, SIEM Segment.

Ping Sweep היא טכניקה לסריקת רשת באמצעות שליחת בקשות ICMP Echo ("ping") למספר כתובות IP כדי לזהות אילו מכשירים ברשת פעילים. זוהי דרך למפות את הרשת. בנוסף ביצענו בדיקה ב-Zenossb ו-Firewall ללא ממצאים חריגים.

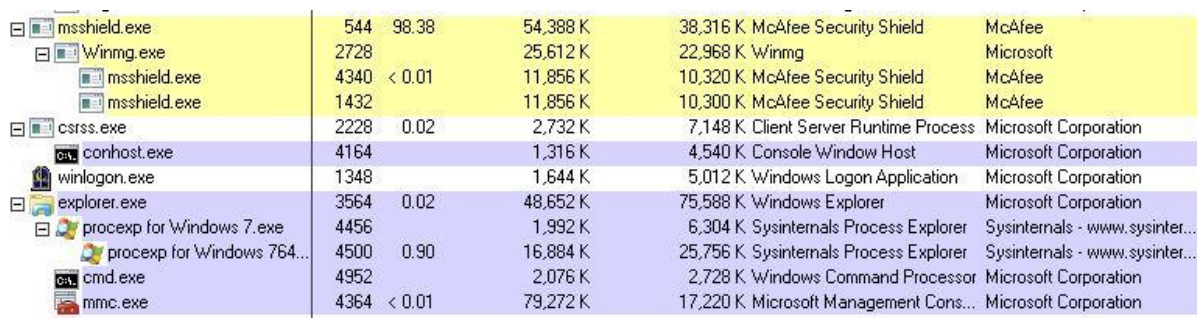
בתמונה צילום מסך של ה-ArcSight:



End Time	Name	Source Address	Destination Address	Source User Name	Destination User Name	Device Address	HostDNSName	Reporter Server
6/23 12:24:26	--Ping Sweep Detected	192.168.200.6				192.168.66.1		ArcsightESM
6/23 12:22:26	--Ping Sweep Detected	192.168.66.20				192.168.66.1		ArcsightESM
6/23 12:22:26	--Ping Sweep Detected	192.168.200.1				192.168.66.1		ArcsightESM
6/23 12:22:26	--Ping Sweep Detected	192.168.200.40				192.168.66.1		ArcsightESM
6/23 12:22:23	--Ping Sweep Detected	192.168.200.100				192.168.66.1		ArcsightESM
6/23 12:22:23	--Ping Sweep Detected	192.168.100.11				192.168.66.1		ArcsightESM
6/23 12:22:19	--Ping Sweep Detected	192.168.200.30				192.168.66.1		ArcsightESM
6/23 12:22:19	--Ping Sweep Detected	192.168.200.23				192.168.66.1		ArcsightESM
6/23 12:21:58	--Ping Sweep Detected	192.168.100.13				192.168.66.1		ArcsightESM
6/23 12:21:58	--Ping Sweep Detected	192.168.100.12				192.168.66.1		ArcsightESM
6/23 12:21:46	--Ping Sweep Detected	192.168.100.10				192.168.66.1		ArcsightESM
7/13 12:39:29	--Privileged Security G...		192.168.200.1			192.168.66.1		ArcsightESM

התחלנו לתחקר את המכונות, נתחיל מהמכונות ב-User Segment, בעיקר כי הן הראשונות. התחלקנו למחשבים וכל אחד בדק מכוונה. לחלקם לא ניתן היה להתחבר, ולמכונות שכן, כשניסנו להיכנס ל-Task Manager בכדי להבין אילו תהליכים רצים במכונה, הוא היה תקוע. בכדי להמשיך בחקירה נרצה להשתמש בכלי Process Explorer של Sysinternals.

העתקנו משרת הקבצים של הארגון CNT-File (192.168.200.6) את התיקיה Sysinternals. הרצנו את Process Explorer וראינו שיש שני קבצים Winmg.exe ו-msshield.exe שמכבידים על ה-CPU ומשתמשים באחוז גבוה ממנו.
 בתמונה צילום מסך של השימוש הגבוה ב-CPU של הקבצים.



Process Name	PID	Private Bytes	Working Set	Company Name	Product Name
msshield.exe	544	98.38 K	54,388 K	McAfee Security Shield	McAfee
Winmg.exe	2728		25,612 K	Winmg	Microsoft
msshield.exe	4340	< 0.01	11,856 K	McAfee Security Shield	McAfee
msshield.exe	1432		11,856 K	McAfee Security Shield	McAfee
csrss.exe	2228	0.02	2,732 K	Client Server Runtime Process	Microsoft Corporation
conhost.exe	4164		1,316 K	Console Window Host	Microsoft Corporation
winlogon.exe	1348		1,644 K	Windows Logon Application	Microsoft Corporation
explorer.exe	3564	0.02	48,652 K	Windows Explorer	Microsoft Corporation
procexp for Windows 7.exe	4456		1,992 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp for Windows 764...	4500	0.90	16,884 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe	4952		2,076 K	Windows Command Processor	Microsoft Corporation
mmc.exe	4364	< 0.01	79,272 K	Microsoft Management Cons...	Microsoft Corporation

נשים לב כי הקבצים הם של חברות McAfee ו-Microsoft, חברות מוכרות וידועות. נמשיך בבדיקת הקבצים. לשם כך השתמשנו בכלי נוסף מ-Sysinternals, בכלי שנקרא Sigcheck, שמטרתו לבדוק חתימות של קבצים, שמות ישנים ועוד.

בבדיקה של הקובץ msshield.exe בכלי ראינו כי הקובץ לא חתום וכי שמו הישן הוא Worm.exe. שני דגלים אלו מעלים חשד, שכן חברה מוכרת וידועה תמיד חותמת את הקבצים שלה, בנוסף השם הישן מעלה חשד רב. ניתן כמעט בוודאות להסיק שהקבצים אינם שייכים לחברות אלו וכי הם זויפו כדי שיראה שהם שייכים לחברות הנ"ל. כמו כן שמו של הקובץ שונה כדי להסיר חשד למי שיבדוק את התוכן.

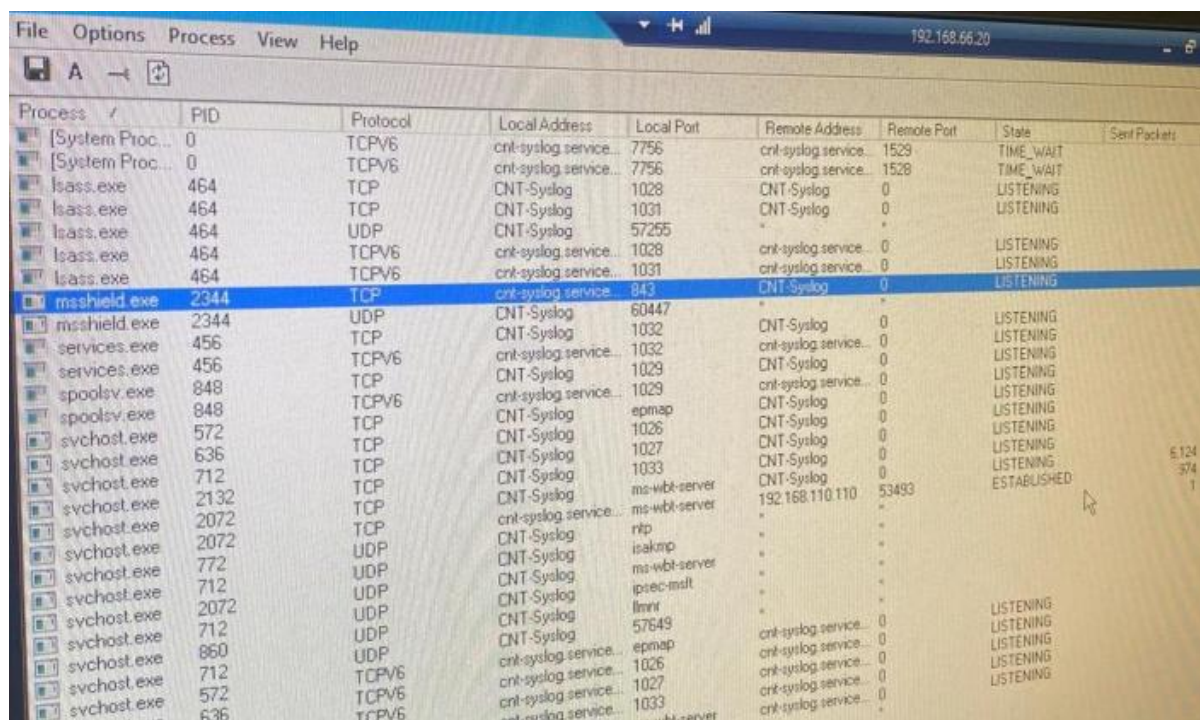
בדקו את שגיאת sigcheck על msshield.

```
C:\Users\administrator.SERVICES\Desktop>sigcheck -a C:\Windows\SysWow64\msshield.exe

Sigcheck v2.73 - File version and signature viewer
Copyright (C) 2004-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\windows\syswow64\msshield.exe:
Verified: Unsigned
Link date: 1:55 PM 7/23/2019
Publisher: n/a
Company: McAfee
Description: McAfee Security Shield
Product: McAfee
Prod version: 1.0.0.0
File version: 1.0.0.0
MachineType: 32-bit
Binary Version: 1.0.0.0
Original Name: Worm.exe
Internal Name: Worm.exe
Copyright: Copyright © McAfee 2012
Comments: McAfee Security Shield
Entropy: 5.416
```

בבדיקה נוספת ב-Process Explorer ראינו כי הקובץ msshield.exe מאזין בפרוטוקול TCP בפורט 843.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets
[System Proc...]	0	TCPV6	cnt-syslog.service...	7756	cnt-syslog.service...	1529	TIME_WAIT	
[System Proc...]	0	TCPV6	cnt-syslog.service...	7756	cnt-syslog.service...	1528	TIME_WAIT	
lsass.exe	464	TCP	CNT-Syslog	1028	CNT-Syslog	0	LISTENING	
lsass.exe	464	TCP	CNT-Syslog	1031	CNT-Syslog	0	LISTENING	
lsass.exe	464	UDP	CNT-Syslog	57255				
lsass.exe	464	TCPV6	cnt-syslog.service...	1028	cnt-syslog.service...	0	LISTENING	
lsass.exe	464	TCPV6	cnt-syslog.service...	1031	cnt-syslog.service...	0	LISTENING	
msshield.exe	2344	TCP	cnt-syslog.service...	843	CNT-Syslog	0	LISTENING	
msshield.exe	2344	UDP	CNT-Syslog	60447			LISTENING	
services.exe	456	TCP	CNT-Syslog	1032	CNT-Syslog	0	LISTENING	
services.exe	456	TCPV6	cnt-syslog.service...	1032	cnt-syslog.service...	0	LISTENING	
spoolsv.exe	848	TCP	CNT-Syslog	1029	CNT-Syslog	0	LISTENING	
spoolsv.exe	848	TCPV6	cnt-syslog.service...	1029	cnt-syslog.service...	0	LISTENING	
svchost.exe	572	TCP	CNT-Syslog	1026	CNT-Syslog	0	LISTENING	
svchost.exe	636	TCP	CNT-Syslog	1027	CNT-Syslog	0	LISTENING	
svchost.exe	712	TCP	CNT-Syslog	1033	CNT-Syslog	0	LISTENING	
svchost.exe	2132	TCP	CNT-Syslog	ms-wbt-server	192.168.110.110	53493	ESTABLISHED	6124
svchost.exe	2072	TCP	cnt-syslog.service...					374
svchost.exe	2072	TCP	CNT-Syslog	ntlp				1
svchost.exe	772	UDP	CNT-Syslog	isakmp				
svchost.exe	712	UDP	CNT-Syslog	ms-wbt-server				
svchost.exe	2072	UDP	CNT-Syslog	ipsec-mgmt				
svchost.exe	712	UDP	CNT-Syslog	lmnr				
svchost.exe	860	UDP	CNT-Syslog	57649	cnt-syslog.service...	0	LISTENING	
svchost.exe	712	TCPV6	cnt-syslog.service...	1026	cnt-syslog.service...	0	LISTENING	
svchost.exe	572	TCPV6	cnt-syslog.service...	1027	cnt-syslog.service...	0	LISTENING	
svchost.exe	636	TCPV6	cnt-syslog.service...	1033	cnt-syslog.service...	0	LISTENING	

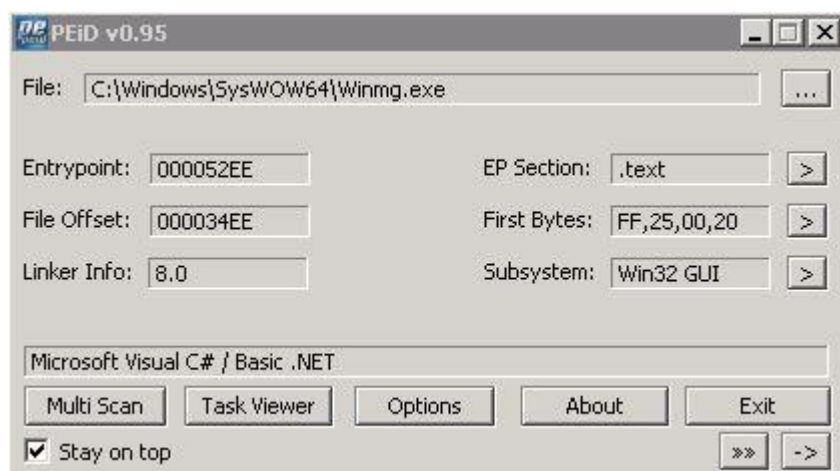
התחברנו באמצעות Telnet לאותו הפורט. ניתן לראות סוג של צ'אט ששואל מי אנחנו וכנראה שמחכה לתשובה מסוימת.

```
C:\> Telnet 192.168.200.1

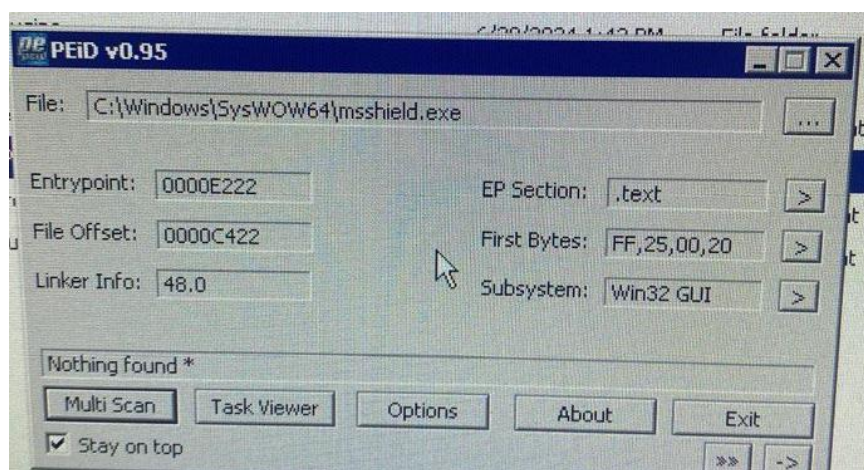
Hi there!
hello
who are you?
Im me
who are you?
DC
who are you?
root
who are you?
admin
who are you?
=
```

המשכנו בחקירת הקבצים. הפעם בעזרת הכלי Peid, שהוא כלי לניתוח קבצים שונים וביניהם קבצי .exe ראינו כי הקובץ Winmg.exe נכתב ב-C# ולעומתו לקובץ msshiel.exe לא הצלחנו למצוא מידע נוסף, אך אנו מניחים שהוא נכתב באופן דומה.

בתמונה שימוש בכלי PEiD על הקובץ 'Winmg.exe':



בתמונה שימוש בכלי PEiD על הקובץ 'msshield.exe':



נשתמש ב-IL DASM כדי לבצע דיסאסמבלינג של הקובץ.

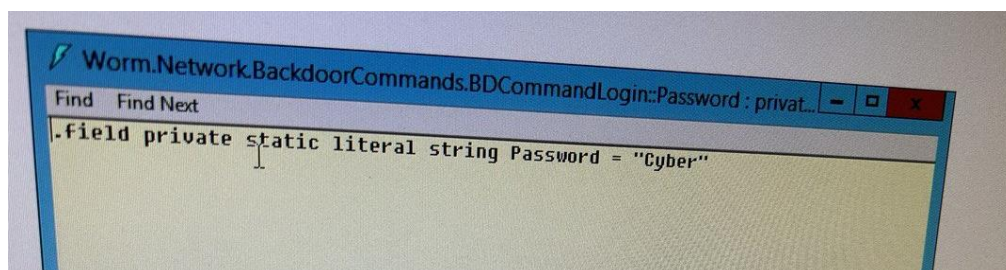
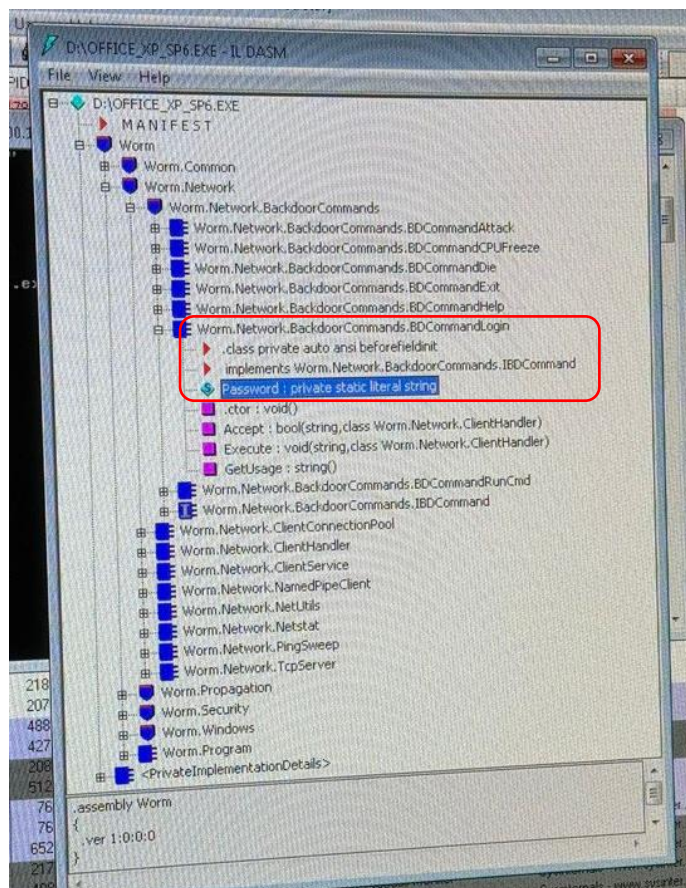
Intermediate Language Disassembler (ILDasm):

הוא כלי מבית מיקרוסופט שמפענח קבצי NET ומראה את הקוד שלהם בשפת הביניים (IL). הכלי מאפשר לראות מבנה של קבצים, כמו מחלקות, שיטות ושדות, ועוזר להבין איך הקוד עובד. ניתן לראות בקובץ בתוך Worm.Networks פונקציות חשודות, כגון TcpServer, Ping Sweep וכן פונקציות CPUFreeze, Attack.

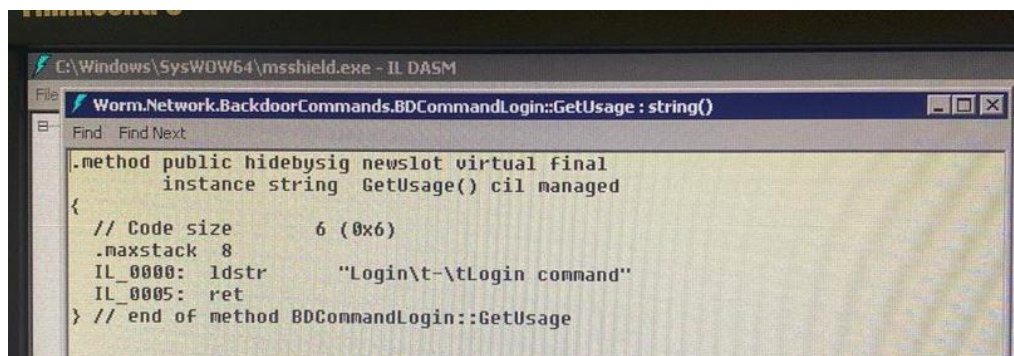
בעצם אנו רואים פה פונקציות שמתאימות לממצאים שמצאנו קודם במערכת: להתראת ה-Ping Sweep, לחיבור ה-TCP ולשימוש הגבוה ב-CPU.

בחיפוש בקבצים תחת המחלקה Backdoor Command ראינו בפונקציה Login כי יש שדה Password שם מצוין כי הסיסמה היא Cyber.

בתמונות ניתן לראות את מיקום השדה בו מצאנו את הסיסמה והתוכן עצמו.

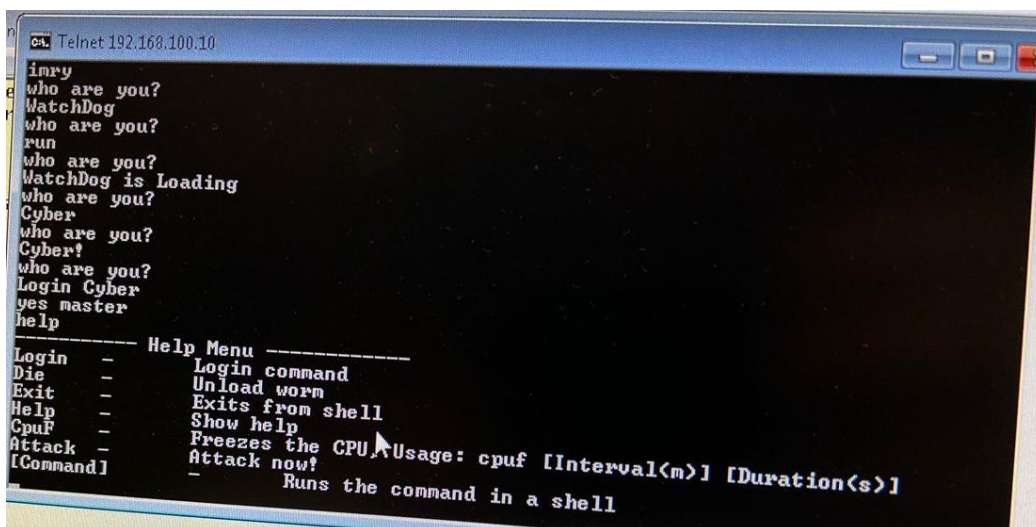


ניסנו להשתמש בסיסמה Cyber כדי להתחבר (דרך ה-Telnet) ללא הצלחה.
נכנסו לפונקציה GetUsage שם ראינו איך להשתמש בסיסמה. בפונקציה נכתב כי בהתחברות צריך לרשום Login ורק אחר כך את הסיסמה.
בתמונה הפונקציה GetUsage.



נסה להתחבר דרך ה-Telnet, הפעם כשאנו יודעים איך ואכן הצלחנו להתחבר. נפעיל את הפקודה help ונשים לב כי מוצעים לנו מספר פקודות זדוניות, שתואמות לפונקציות שראינו ב-ILDASM.

בתמונה זו אפשר לראות את הפקודה שמפעילה את הקפאה המעבד, כפי שראינו קודם.

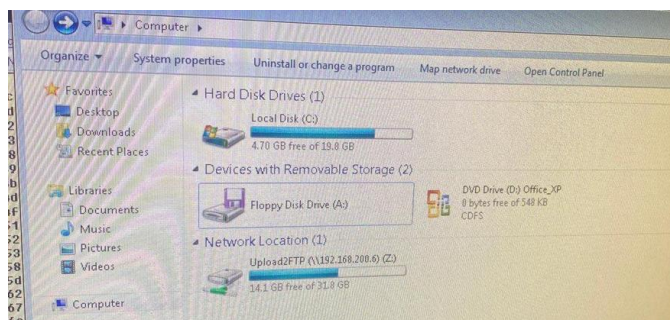


```

C:\ Telnet 192.168.100.10
imry
who are you?
WatchDog
who are you?
run
who are you?
WatchDog is Loading
who are you?
Cyber
who are you?
Cyber!
who are you?
Login Cyber
yes master
help
-----
Login - Login command
Die - Unload worm
Exit - Exits from shell
Help - Show help
CpuF - Freezes the CPU Usage: cpuf [Interval<m>] [Duration<s>]
Attack - Attack now!
[Command] - Runs the command in a shell
  
```

כמו כן, ניתן להבחין כאן בבירור ששרת השליטה ובקרה של התוקף מאפשר שליטה מרחוק והפעלת פקודות זדוניות. זהו השלב שבו אנו מפלילים בבירור את הקובץ.

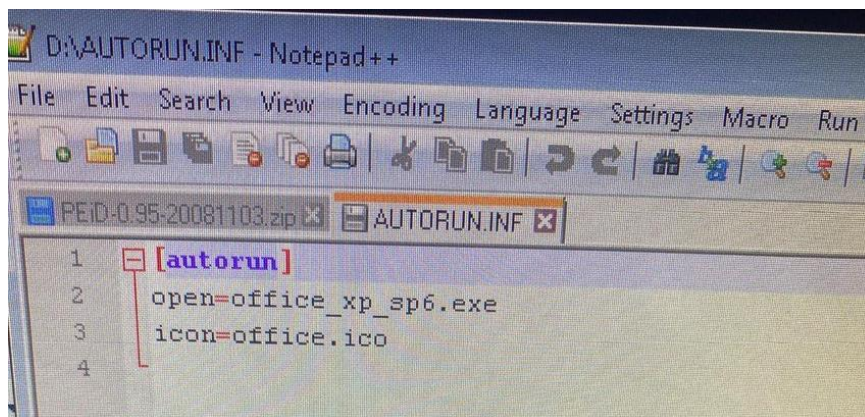
נמשיך בבירור התקיפה וננסה להבין איך הקבצים האלו הוחדרו למערכת. המכונה הראשונה שה-ArcSight התריע על Ping Sweep היא 192.168.100.10 ועל כן התחלנו לתחקר אותה. ראינו בהתקנים המחוברים כי למחשב מחובר כונן דיסקים שבו יש דיסק בשם Office_XP.



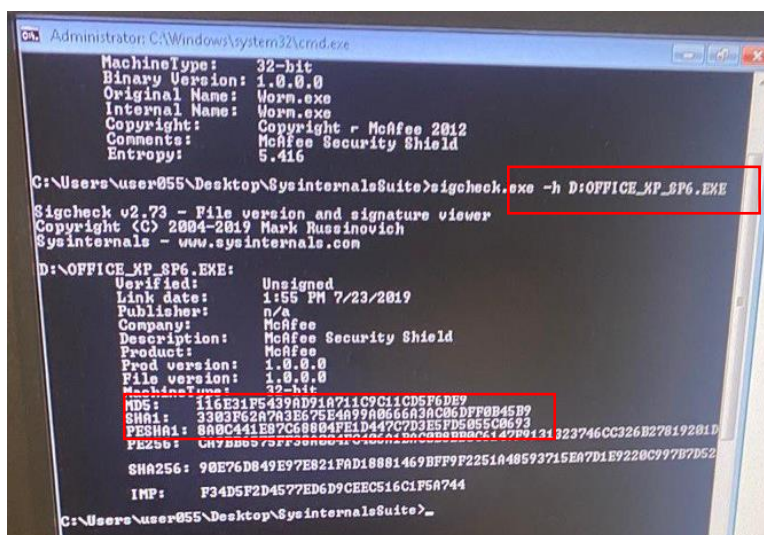
נפתח כמובן ללא הרצה את תיקיית ה-DVD, שם ראינו כי ישנם שלושה קבצים- קובץ הרצה שנקרא SP_XP_OFFICE 6, קובץ בשם AUTORUN ואייקון של OFFICE.

Name	Date modified	Type	Size
Files Currently on the Disc (3)			
AUTORUN	6/30/2024 11:30 AM	Setup Information	1 KB
OFFICE	6/30/2024 11:30 AM	Icon	107 KB
OFFICE_XP_SP6	6/30/2024 11:30 AM	Application	88 KB

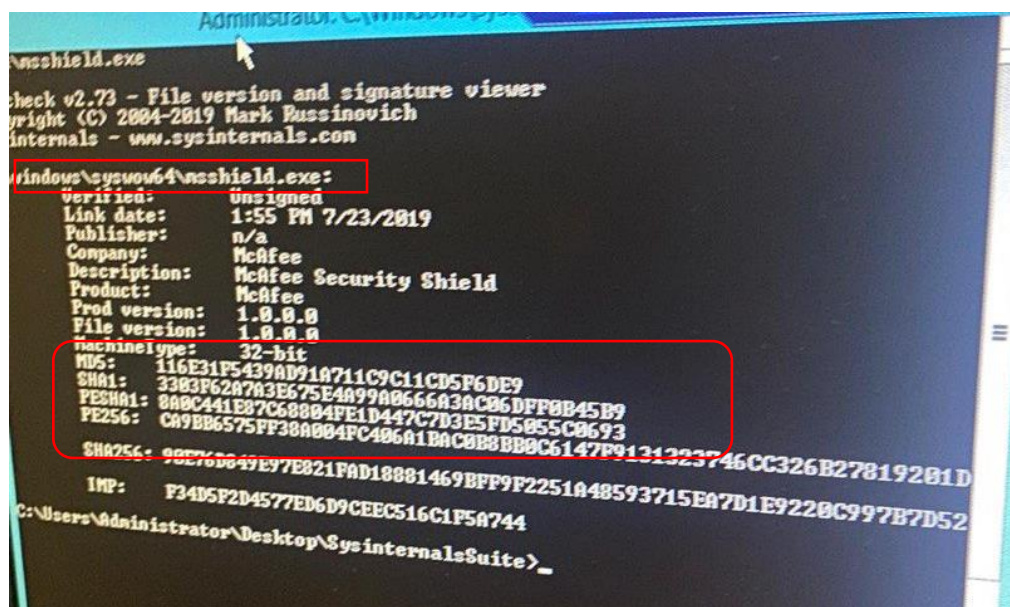
אנו חושדים שזהו איננו קובץ של OFFICE שכן קובץ הרצה של אופיס שוקל יותר מ-88 KB. פתחנו את קובץ ה-AUTORUN, נוכל לראות כי הוא מוגדר להריץ את הקובץ SP_XP_OFFICE 6, ואת האייקון של אופיס.



כדי לבדוק את הקובץ השתמשנו שוב בכלי sigcheck של Sysinternals. מבדיקה של MD5 ו-SHA ראינו כי הקובץ הנ"ל והקובץ msshield.exe זהים (Hash זהה).
בתמונה Sigcheck של קובץ ה-OFFICE.

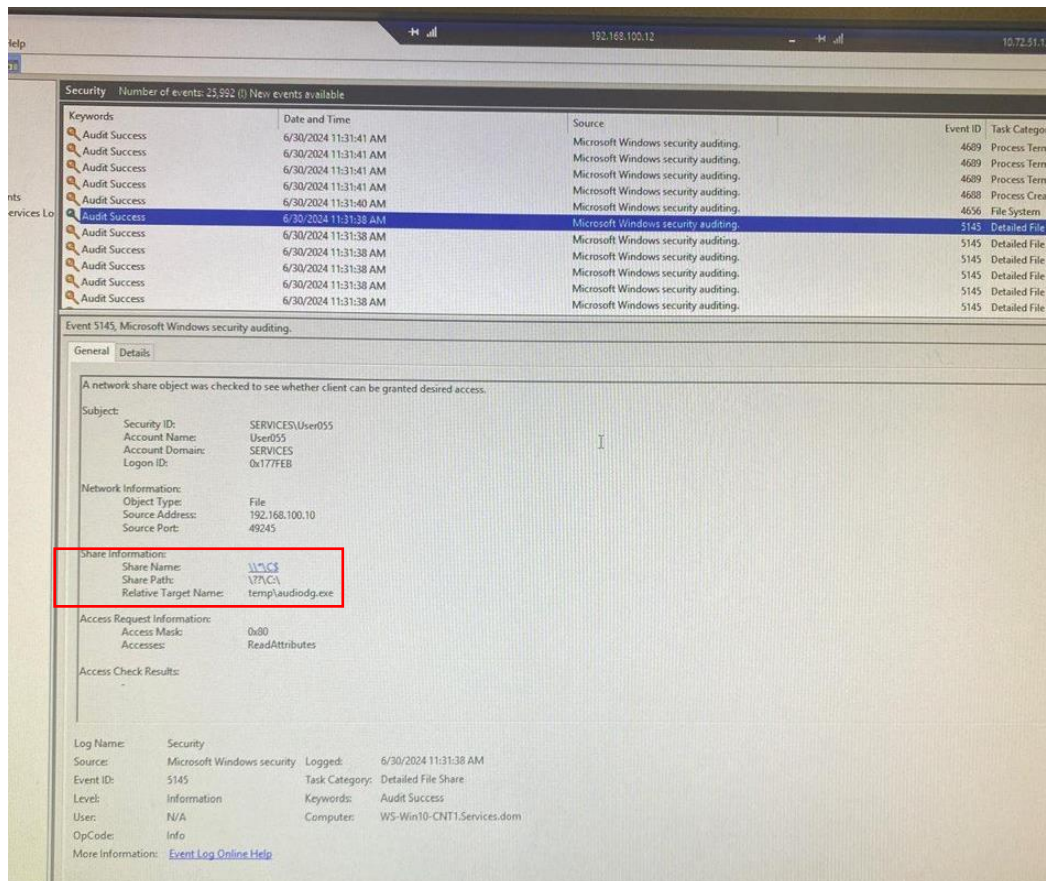


בתמונה Sigcheck של קובץ msshield.exe.



כעת אנו מסיקים כי מכונה זו היא המכונה הראשונה שהודבקה בקובץ. ננסה להבין איך שאר המכונות קיבלו את הקובץ.

נכנס ל-EventViewer במכונה זו 192.168.100.10 ונחפש תנועה של קבצים. ראינו שיש פרוטוקול בשם SMB המאפשר שיתוף קבצים בין מכונות Windows. בסיון לפי פרוטוקול SMB מצאנו כי המכונה שלנו שלחה למכונה 192.168.100.12 את הקובץ audiodg.exe.



בדקנו את החתימה של הקובץ בעזרת Sigcheck וראינו כי ה-MD5 שלו זהה, כלומר זהו אותו קובץ זדוני.

מכאן מצאנו את דרך ההפצה של הקובץ הזדוני בין המכשירים. ההפצה קרתה דרך שליחה ממכונה למכונה דרך שליחת קבצים בפרוטוקול SMB.


```
C:\Users\User067\Desktop\SysinternalsSuite>sigcheck.exe -h "C:\temp\audiodg.exe"

Sigcheck v2.73 - File version and signature viewer
Copyright (C) 2004-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\temp\audiodg.exe:
Verified: Unsigned
Link date: 1:55 PM 7/23/2019
Publisher: n/a
Company: McAfee
Description: McAfee Security Shield
Product: McAfee
Prod version: 1.0.0.0
File version: 1.0.0.0
MachineType: 32-bit
MD5: 116E31F5439AD91A711C9C11CD5F6DE9
SHA1: 3303F62A7A3E675E4A99A0666A3AC06DFF0B45B9
PESHA1: 8A0C441E87C68804FE1D447C7D3E5FD5055C08693
PE256: CAC800573FF38A084FC406A1BAC0B8880C6147F9131323746CC326B27819201D
SHA256: 90E76D849E97E821FAD188814698FF9F2251A48593715EA7D1E9220C99787B7D52
IMP: F34D5F2D4577ED6D9CEEC516C1F5A744

C:\Users\User067\Desktop\SysinternalsSuite>sigcheck.exe -a "C:\temp\audiodg.exe"

Sigcheck v2.73 - File version and signature viewer
Copyright (C) 2004-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\temp\audiodg.exe:
Verified: Unsigned
Link date: 1:55 PM 7/23/2019
Publisher: n/a
Company: McAfee
Description: McAfee Security Shield
Product: McAfee
Prod version: 1.0.0.0
File version: 1.0.0.0
MachineType: 32-bit
Binary Version: 1.0.0.0
Original Name: Worm.exe
Internal Name: Worm.exe
Copyright: Copyright - McAfee 2012
Comments: McAfee Security Shield
```

3. פירוק ווקטור התקיפה לשלבים לפי MITRE:

- A. [Reconnaissance](#): לא זוהה שלב זה. לא מצאנו ראיות לאיסוף מידע מקדים של התוקף. ניתן להניח כי התוקף חקר כיצד לבצע את ההכנסה הפיזית של הדיסק לארגון.
- B. [Resource Development](#): התוקף ייצר את קובץ ה-Worm.exe, את הקובץ שירץ אותו AUTORUN והשתיל אותם בתוך דיסק.
- C. [Initial Access](#): התוקף הצליח להכניס את הדיסק למכונה בארגון. לא ברור איך אבל זוהי הגישה הראשונית, ומשם הקובץ הופץ לשאר המכונות עי שליחה ב-SMB.
- D. [Execution](#): כשהדיסק מוכנס למחשב, קובץ ה-AUTORUN מריץ את הקובץ הזדוני OFFICE_XP_S86. אז התבצע Ping Sweep שמטרתו לזהות מכונות בארגון. משם הקובץ שותף למכונות אחרות בארגון בפרוטוקול SMB. הקובץ הזדוני בעצם מאפשר לתוקף להקפיד את ה-CPU באמצעות שרת שליטה ובקרה מרחוק.
- E. [Persistence](#): התוקף מפעיל שרת שליטה ובקרה מרחוק (דרך קשר TCP בפורט 843), ובאמצעות השרת הוא מעלה את השימוש במעבד, מה שגורם לכך שלא ניתן להשתמש ב-Task Manager שמשם ניתן בקלות להבין מה התהליך שתוקע את המחשב ולסיים אותו. בנוסף, כל עוד הדיסק בתוך מכונה 10, בכל פעם שהדיסק יטען מחדש התקיפה תתבצע בשנית. אנו מניחים כי גם בעת הפעלה מחדש של המכונות (בשביל לסיים את התהליכים שתוקעים את ה-CPU), הדיסק יטען מחדש, אם כי לא בדקנו זאת.
- F. [Privilege Escalation](#): באופן פשוט של השלב, התוקף לא עשה פעולות כדי להשיג הרשאות גבוהות יותר. אם כי בראייה רחבה התוקף הצליח לחדור למכונה אחת באופן פיזי, ומשם הצליח להריץ פקודות מערכת במספר רב של מכונות, כולל מכונות חשובות בארגון.

- G. [Defense Evasion](#): התוקף התחזה לקבצים לגיטימיים של Microsoft ו-McAfee כדי להימנע מזיהוי ושינה את שמות הקבצים באופן שלא יעורר חשד (Office_xp_s86,mssield). כמו כן התוקף מנע גישה ל-Task Manager כך לא נראה את התהליכים שגורמים למעבד לקפוא.
- H. [Credential Access](#): לא זוהה שלב זה, לא ראינו גניבת סיסמאות.
- I. [Discovery](#): התוקף השתמש ב-Ping Sweep כדי לזהות מכונות נוספות בארגון.
- J. [Lateral Movement](#): התוקף חדר באופן פיזי למכונה 10, ומשם הפיץ את הקובץ למכונות נוספות רבות בארגון באמצעות שליחת הקובץ אליהם.
- K. [Collection](#): לא זיהינו איסוף מידע מלבד Ping Sweep שמטרתו להבין לאילו מכונות ניתן להפיץ את הקובץ הזדוני.
- L. [Command and Control](#): התוקף מתקין שרת שליטה ובקרה במכונות שנדבקו בקובץ (בכל מכונה ומכונה), באמצעות שרת על TCP בפורט 843. מה שמאפשר לו לשלוט מרחוק במערכת על ידי התחברות בסיסמה, ולהפעיל פקודות מערכת זדוניות.
- M. [Exfiltration](#): לא זוהתה הזלגת מידע מהארגון.
- N. [Impact](#): המכונות בארגון איטיות מאוד בעקבות הקפאת ה-CPU עד כדי שלא ניתן להשתמש בהם. בעצם ניתן להגיד שחלק גדול מהארגון עלול לא לתפקד בעקבות ההשבתה או האטה משמעותית של המכונות הנגועות.
4. מידע תקשורתי:
- הצד התקשורתי אינו חלק משמעותי בתקיפה, אם כי חלק מההתקפה כללה שימוש בתקשורת. לאחר שהתוקף התחבר פיזית למכונה 10 ב-User Segment הוא ביצע Ping Sweep בכדי לסרוק את הארגון ולמצוא מכונות נוספות שניתן לשלוח אליהן את הקובץ הזדוני. לאחר שגילה מכונות נוספות, שלח אליהם את הקובץ באמצעות פרוטוקול SMB. התוקף שלט במכונות שהותקפו עי שרת שליטה ובקרה על פרוטוקול TCP בפורט 843.
5. פעולות לוקאליות:
- A. המשתמש שדרכו נכנס התוקף: התוקף הצליח להכניס דיסק לכונן הדיסקים במכונה 192.168.100.10 ומשם למכונות נוספות בארגון ע"י שליחת הקובץ.
- B. קבצים שנפגעו/שוננו/הועתקו/הושטלו: התוקף החדיר קובץ זדוני שגורם לפי סדר הפעולות שתיארנו להקפאת המעבד. ראינו את ההשפעה של ההקפאה על פעילות ה-Task Manager, על איטיות המכונות וייתכן שישנה השפעה גם לתוכניות/תוכנות נוספות. שם הקובץ הזדוני הוא Worm אך הוא מופיע במספר שמות שונים כדי שלא נזהה אותו.
- C. מסקנות נוספות: הפרצה הראשונית בתקיפה הייתה דרך חיבור פיזי למכונה בארגון, מה שגרם לפגיעה משמעותית בארגון. מכאן אנו למדים על חשיבות האבטחה הפיזית בארגון, כיון שפעולה כה פשוטה גרמה לנזק משמעותי לארגון.
6. הגנה:
- A. הגנה ראשונית: הוצאת הדיסק ממכונה 192.168.100.10 - חסימת השרת ע"י התחברות ב-Telnet לשרת וכתביה הפקודה Die, לחסום את פורט 843, לסיים את פעולות התהליך. -להכניס rule לאנטי וירוס שלא יאפשר את הקובץ הזדוני (בדיקת Hash).

B. הגנה מניעתית :

-הדרכת המשתמשים בארגון לשימוש נכון ובטוח בהתקנים פיזיים. ניתן לשקול איסור על הכנסת התקנים פיזיים לארגון במידת האפשר.
-הוספת כלל לאנטי וירוס על בדיקה של תהליכים שצורכים כמות גבוהה של CPU או שאר המשאבים.
(לציין כי לא נרצה לחסום מידית, אלא בעיקר להתריע, מאחר שישנם תהליכים שצורכים כמות גבוהה של משאבים והם לגיטימיים).
-בקרה על שיתוף קבצים בארגון, בין אם ע"י בדיקה שלהם או רק עם הרשאה מיוחדת. בפרט חסימה או הגבלה על שליחת קבצי exe, בין אם בפרוטוקול SMB או בשאר הדרכים לשליחת קבצים בארגון.

7. הערות נוספות :

A. אופן עבודת הצוות :

האירוע נוהל בצורה טובה, תרחיש שהצריך חשיבה משותפת ושיתוף פעולה רב.

B. מגבלות העבודה :

במהלך התרחיש היה שימוש בכלים שלא השתמשנו בהם בעבר, ועם הדרכה הצלחנו להשתמש בהם.