27.8.22

Final Assignment

Remote Access Trojan (RAT)

מבוא:

RAT's מייצגים תוכנות זדוניות המאפשרות ניטור, שליטה וניהול מרחוק על מחשב או על רשת מחשבים.

כיום על מנת לקבל שירות ממחלקת התמיכה הטכנית בארגון או בבית עבור המחשב אין צורך להגיע פיזית אל המחשב של המשתמש, קיימת גישה מרחוק, כאשר היא מופעלת, מחשבים ושרתים מורשים יכולים לשלוט בכל מה שקורה במחשב שלך. יכולת לפתוח מסמכים, הרצת תוכנות וכו' בזמן אמת.

RAT הוא סוג של תוכנה זדונית הדומה מאוד לתוכנות גישה מרחוק. ההבדל העיקרי, הוא ש RAT's מותקנים במחשב ללא ידיעת המשתמש. רוב תוכנות הגישה מרחוק מיוצרות למטרות תמיכה טכנית ושיתוף קבצים, בעוד ש-RAT's מיועדות לריגול כגון יכולת להפעיל את מצלמת האינטרנט או המיקרופון של המחשב בדיסקרטיות. השתלטות על רשתות ויצירה של רשת בוטים ובכך מאפשרת ניצול של משאבי המחשבים למתקפות כמו DDOS, כרייה של מטבעות וירטואליים (רשת בוטים שמורכבת מאלפי מחשבים יכולה לייצר הרבה כסף).

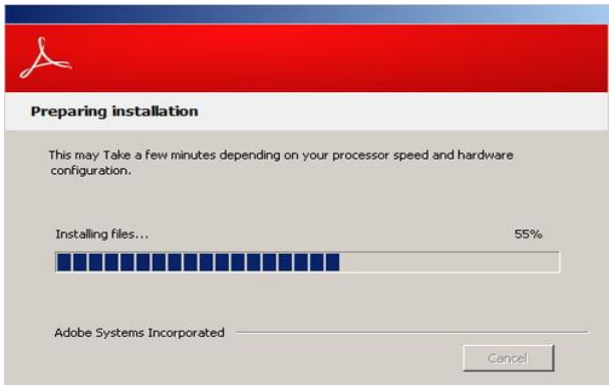
RAT's כוללים קבצים בעלי מראה לגיטימי. האקרים יכולים לצרף RAT's למסמך בדוא"ל, או בתוך קבצים גדולים, כמו משחק מחשב. פרסומות ודפי אינטרנט מפוקפקים, למרות שרוב הדפדפנים מונעים הורדות אוטומטיות מאתרים או מודיעים למשתמש כאשר אתר אינו בטוח.

שלא כמו תוכנות זדוניות ווירוסים מסוימים, ייתכן שיהיה קשה לדעת מתי התבצעה הורדה של RAT's. הימצאות התוכנות הזדוניות אלו לא יאטו את המחשב, והאקרים לא תמיד יסגירו את עצמם על ידי מחיקת הקבצים הזדוניים או גלגול הסמן סביב המסך. במקרים מסוימים, משתמשים נדבקים על ידי RAT's במשך שנים מבלי לשים לב לשום דבר שהוא לא בסדר.

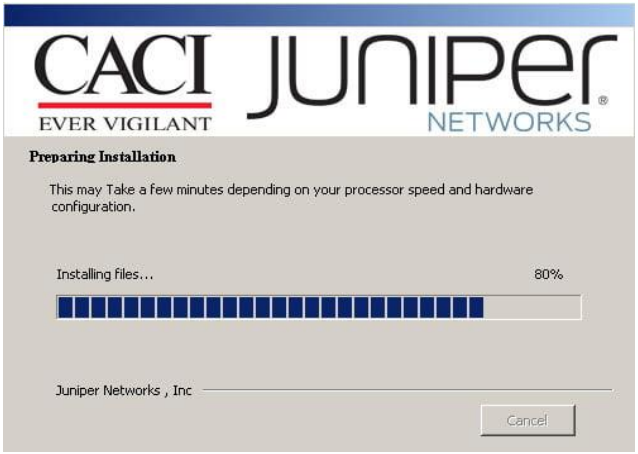
על מנת להבין יותר טוב את מנגנון הפעולה נחקור לדוגמא תוכנה זדונית בשם "SAKULA":

"SAKULA"/"Sakurel" - סוס טרויאני שהופץ לראשונה ע"י קבוצת האקרים סינית בשם "Deep Panda" הידועה כקבוצה הפוגעת בתעשיות רבות, ממשל, ביטחון, וכלכלה. התוכנה מאפשרת גישה מרחוק, ברגע שמתבצעת הדבקה היא אינה מראה סימן כלשהו במכונה הנגועה, שיטות ההפצה העיקריות הן דרך קמפיינים של דואר זבל, קבצי pdf, מקורות הורדת תוכנות לא מהימנים, סוסים טרויאנים נוספים שמורידים ומתקינים תוכנות זדוניות אחרות ועדכוני תוכנה מזויפים. בין הנזקים העיקרים: גניבה של סיסמאות, זהויות, הפיכה של המחשב לבוטנט.

דוגמאות לדרכי הפצה של התוכנה הזדונית "SAKULA"



איור 1: צילום מסך של Adobe, שלמעשה מתקין את התוכנה SAKULA



איור 2: צילום מסך של התקנת Juniper, שלמעשה מתקין את התוכנה "SAKULA"

Miter Attack

טבלה מס' 1: זיהוי הטכניקות ב"MITER ATTACK"

Execution	Persistence	Privilege Escalation	Defense Evasion	Lateral Movement	Command And Control
Command-Line Interface	New Service	Bypass User Account Control	Bypass User Account Control	Remote File Copy	Custom Cryptographic Protocol
Rundll32	Registry Run Keys / Startup Folder	New Service	DLL Side-Loading		Remote File Copy
			File Deletion		Standard Application Layer Protocol
			Obfuscated Files or Information		
			Rundll32		

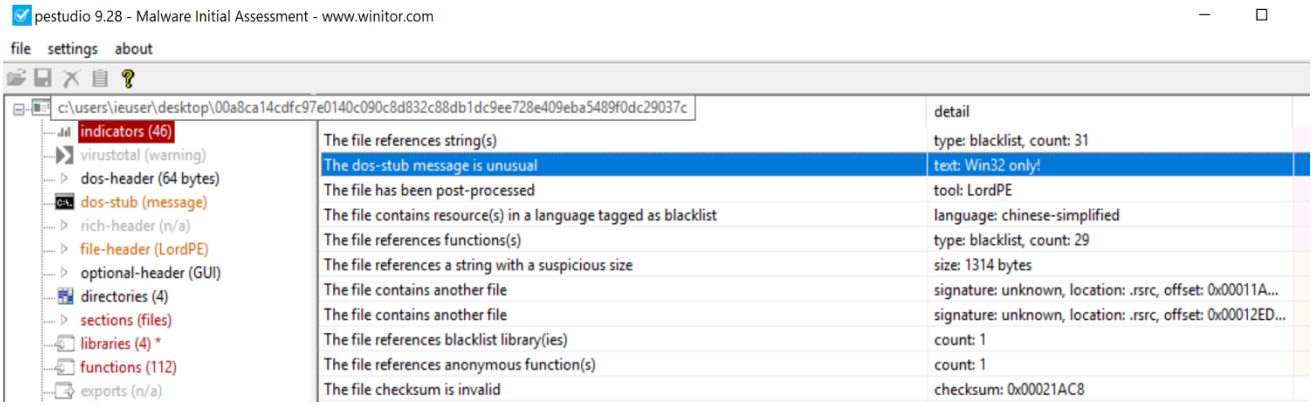
עפ"י טבלה מס' 1 ניתן לומר שהתוכנה הזדונית משתמשת במספר טכניקות:

1.ברמת הביצוע כאשר התוכנה מורדת ע"י המשתמש היא יוצרת אינטראקציה דרך ממשק שורת הפקודה, נוצרים שירותים חדשים, מפתחות הפעלה של רישום, תיקיית אתחול, כל אלו גורמים לתוכנית לפעול בכל פעם שהמשתמש נכנס למכונה.
2.הסלמת הרשאות ניצול של טכניקה זו מאפשר לתוכנה לקבל הרשאות ברמה הגבוה ביותר, שליטה על חשבונות משתמשים והפעלה של עוד שירותים חדשים שמתאפשרים כעת לאחר ההסלמה.
3. התחמקות מהגנה- החלפת סיסמאות משתמשים, קימפול של הקוד הזדוני בקבצי DLL והטענתם, מחיקה של הקובץ הזדוני/ שינוי של קבצים על מנת לשבש כל תוכנת הגנה שלא תהיה על המכונה הנגועה וכך להבטיח שרידות.
4. תנועה רוחבית- העברת קבצים מרחוק עוזרת בהוספה של כלים נוספים לרשת הקורבן שאינם קיימים. ובכך ניתן להרחיב את התקיפה.
5.שליטה ובקרה – קביעה ושליטה על סוג ההצפנה, הגדרת אופן העברה וסוגים שונים של הודעות שרת לקוח, הפועלים על מערכות קצה שונות, בפרוטוקול שכבת יישומים.

27.8.22

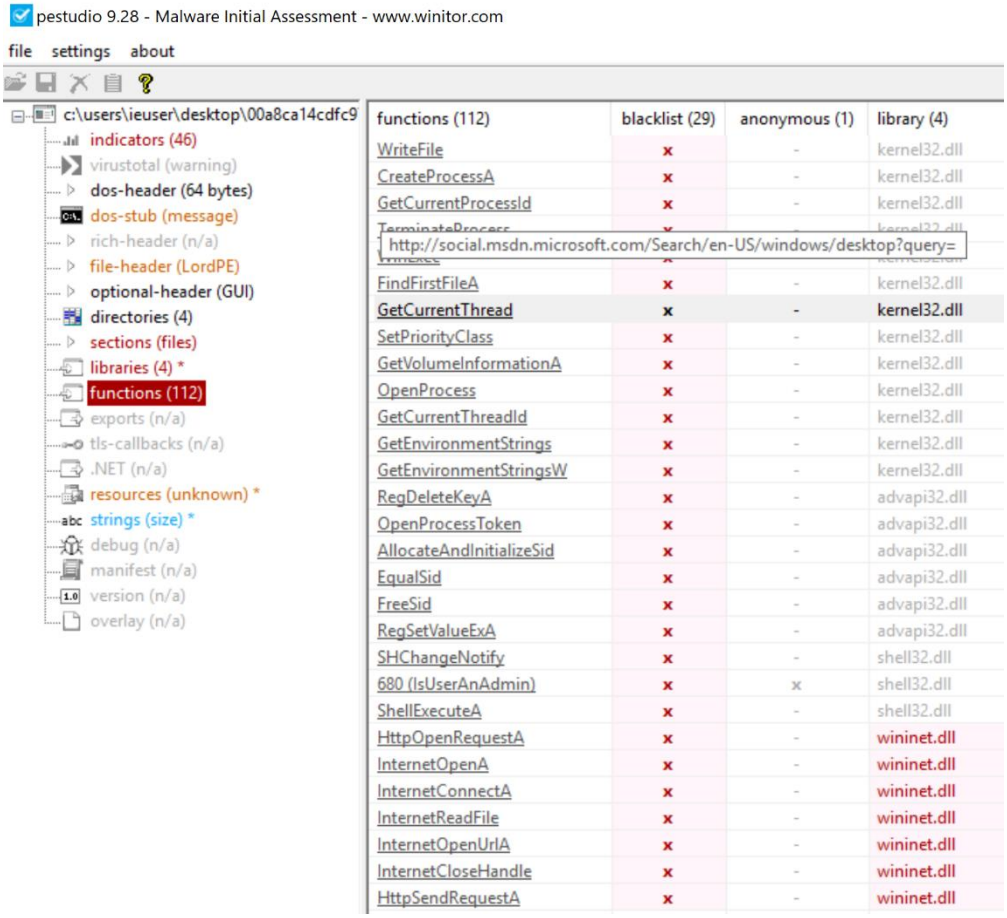
Malware Analysis

Static analysis



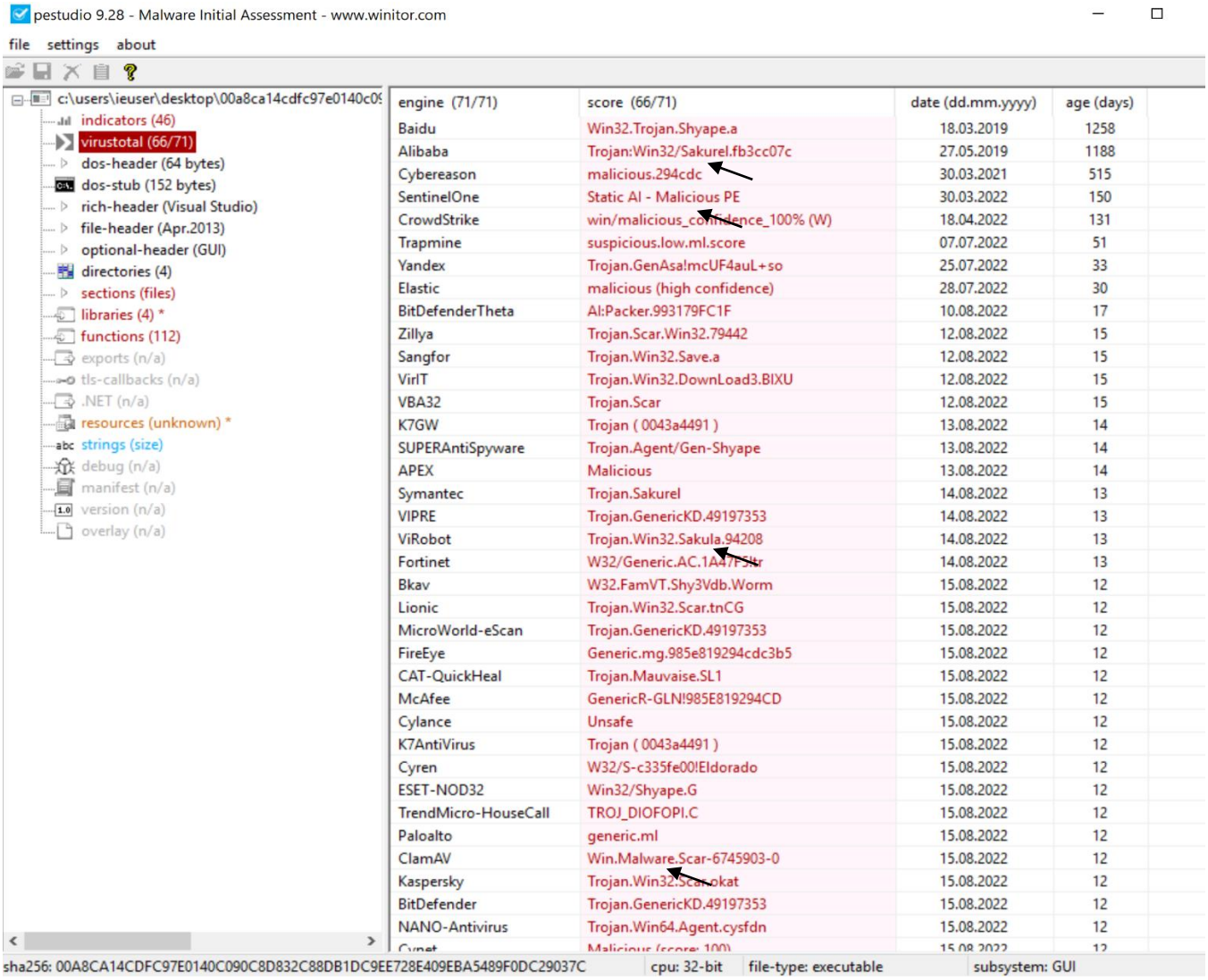
איור 3: ניתוח כללי של הקובץ הזדוני בעזרת הכלי "pestudio".

תחת הרשימה השחורה, נמצאו 31 מחרוזות, 29 פונקציות, השפה העיקרית שהקבצים כתובים בה היא סינית.



איור 4: ניתוח של פונקציות מתוך הקובץ הזדוני בעזרת הכלי "pestudio"

ניתן להבחין במספר פונקציות שמיד מרמזות לנו על מה שהקובץ עושה כגון: "WriteFile", "CreateProccessA", "OpenProccess" כל הפונקציות מתקשרות לטכניקות התקיפה שהוזכרו קודם לכן ב- "MITER ATTACK".



engine (71/71)	score (66/71)	date (dd.mm.yyyy)	age (days)
Baidu	Win32.Trojan.Shyape.a	18.03.2019	1258
Alibaba	Trojan:Win32/Sakurel.fb3cc07c	27.05.2019	1188
Cybereason	malicious.294cdc	30.03.2021	515
SentinelOne	Static AI - Malicious PE	30.03.2022	150
CrowdStrike	win/malicious_confidence_100% (W)	18.04.2022	131
Trapmine	suspicious.low.ml.score	07.07.2022	51
Yandex	Trojan.GenAsa!mcUF4auL+so	25.07.2022	33
Elastic	malicious (high confidence)	28.07.2022	30
BitDefenderTheta	AI:Packer.993179FC1F	10.08.2022	17
Zillya	Trojan.Scar.Win32.79442	12.08.2022	15
Sangfor	Trojan.Win32.Save.a	12.08.2022	15
VirIT	Trojan.Win32.DownLoad3.BIXU	12.08.2022	15
VBA32	Trojan.Scar	12.08.2022	15
K7GW	Trojan (0043a4491)	13.08.2022	14
SUPERAntiSpyware	Trojan.Agent/Gen-Shyape	13.08.2022	14
APEX	Malicious	13.08.2022	14
Symantec	Trojan.Sakurel	14.08.2022	13
VIPRE	Trojan.GenericKD.49197353	14.08.2022	13
ViRobot	Trojan.Win32.Sakula.94208	14.08.2022	13
Fortinet	W32/Generic.AC.1A47F3!tr	14.08.2022	13
Bkav	W32.FamVT.Shy3Vdb.Worm	15.08.2022	12
Lionic	Trojan.Win32.Scar.tnCG	15.08.2022	12
MicroWorld-eScan	Trojan.GenericKD.49197353	15.08.2022	12
FireEye	Generic.mg.985e819294cdc3b5	15.08.2022	12
CAT-QuickHeal	Trojan.Mauvaise.SL1	15.08.2022	12
McAfee	GenericR-GLN!985E819294CD	15.08.2022	12
Cylance	Unsafe	15.08.2022	12
K7AntiVirus	Trojan (0043a4491)	15.08.2022	12
Cyren	W32/S-c335fe00!Eldorado	15.08.2022	12
ESET-NOD32	Win32/Shyape.G	15.08.2022	12
TrendMicro-HouseCall	TROJ_DIOFOPI.C	15.08.2022	12
Paloalto	generic.ml	15.08.2022	12
ClamAV	Win.Malware.Scar-6745903-0	15.08.2022	12
Kaspersky	Trojan.Win32.Scar.pkat	15.08.2022	12
BitDefender	Trojan.GenericKD.49197353	15.08.2022	12
NANO-Antivirus	Trojan.Win64.Agent.cysfdn	15.08.2022	12
Cynet	Malicious (score: 100)	15.08.2022	12

איור 5: ניתוח של virustotal מתוך הכלי "pestudio"

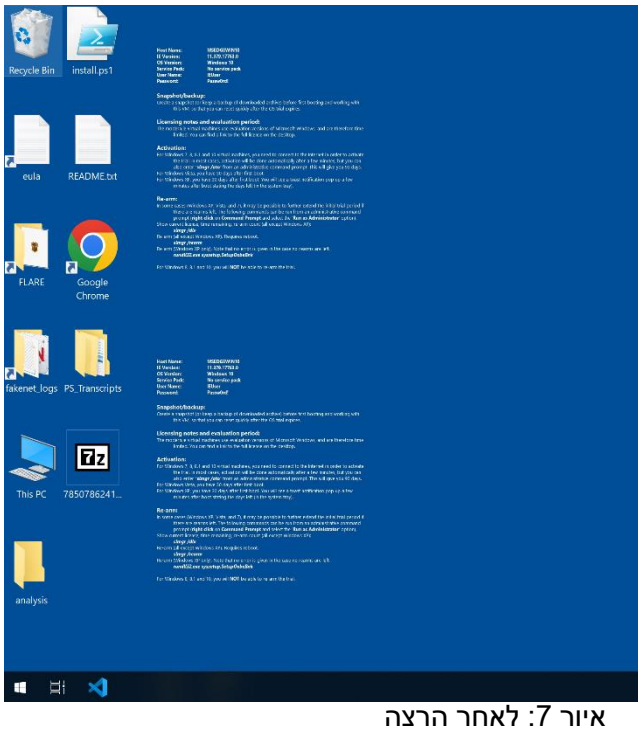
בהמשך לאיור 7 ישנם כמה חתימות שחוזרות על עצמן/ מעלות חשד לגבי התוכנה הזדונית, מה שמחזק את הטענה לגבי הקובץ כי הוא מהווה איום ממשי.

מילים כמו "Malware", "Malicious", ואפילו השם של התוכנה כפי שתואר בתחילת הדו"ח "Sakurel"(שם נוסף), "Sakula".

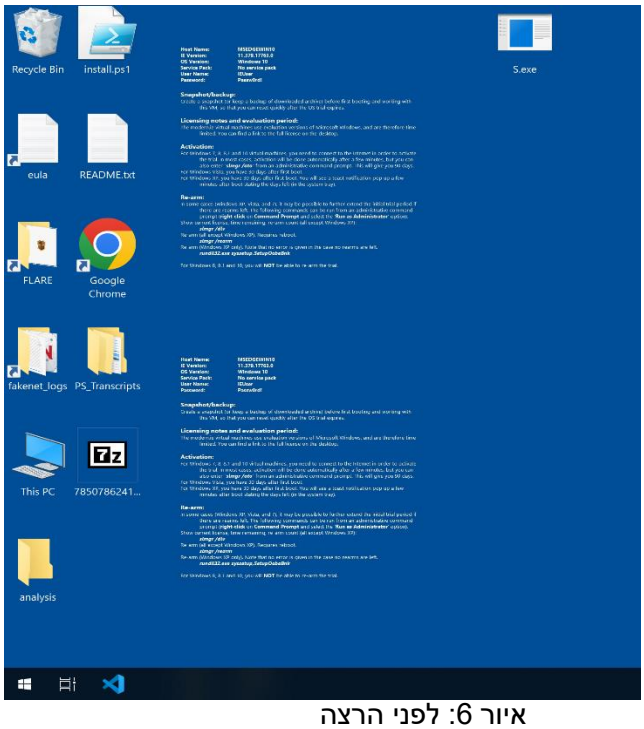
27.8.22

Dynamic Analysis

מחיקת הקובץ כחלק מהתחמקות מהגנה

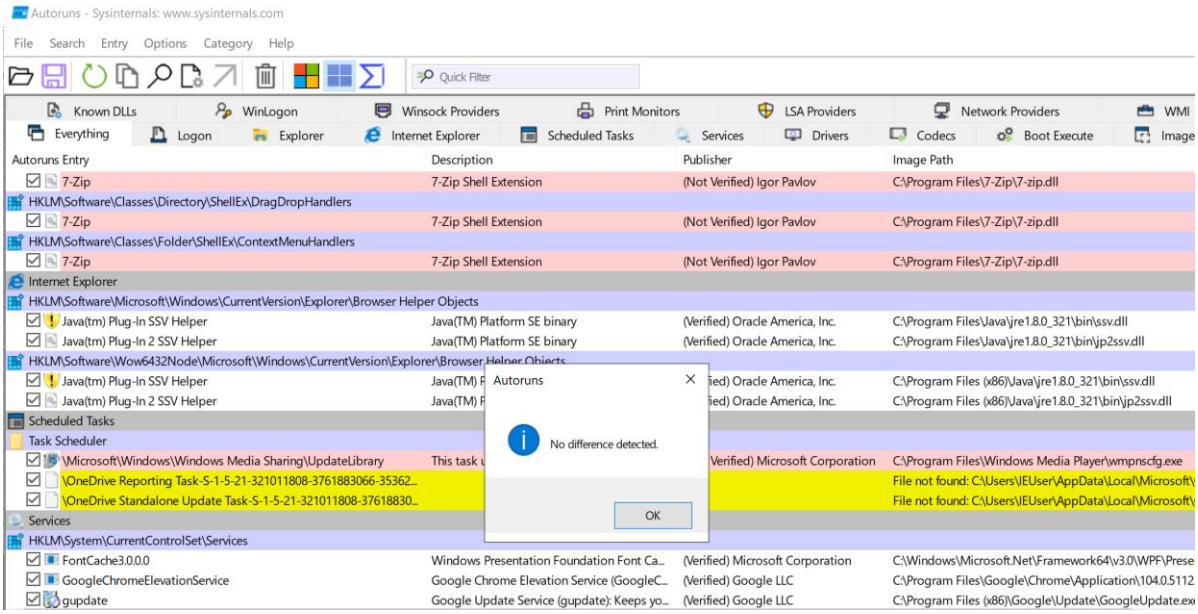


איור 7: לאחר הרצה



איור 6: לפני הרצה

מיד לאחר הרצת הקובץ במכונה הווירטואלית, שמתי לב שהקובץ נעלם, התוכנה הזדונית מפעילה טכניקה של התחמקות מהגנה על ידי מחיקת קבצים כך שהמשתמש אינו יודע על כך שנדבק.



איור מס' 8- איחוד התוצאות לפני ואחרי הרצת הקובץ בכלי "Autoruns"

לא נמצאו הבדלים, אפשר להסביר זאת שוב ע"י טכניקת התחמקות שכן הקובץ מוחק את עצמו לאחר ההפעלה.

27.8.22

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
6:37:58.9860168 AM	S.exe	4188	Process Start		SUCCESS	Parent PID: 4284, Command line: "C:\Users
6:37:58.9860218 AM	S.exe	4188	Thread Create		SUCCESS	Thread ID: 1404
6:37:59.0154872 AM	S.exe	4188	Load Image	C:\Users\IEUser\Desktop\S.exe	SUCCESS	Image Base: 0x400000, Image Size: 0x190
6:37:59.0155234 AM	S.exe	4188	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffb41050000, Image Size:
6:37:59.0155459 AM	S.exe	4188	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x778b0000, Image Size: 0x1
6:37:59.0156359 AM	S.exe	4188	CreateFile	C:\Windows\Prefetch\S.EXE-E3F52F9A.pf	NAME NOT FOUND	Desired Access: Generic Read, Dispositior
6:37:59.0157867 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value
6:37:59.0157977 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
6:37:59.0158097 AM	S.exe	4188	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\Rais...	NAME NOT FOUND	Length: 80
6:37:59.0158184 AM	S.exe	4188	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
6:37:59.0158314 AM	S.exe	4188	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Se...	REPARSE	Desired Access: Query Value
6:37:59.0158385 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Seg...	NAME NOT FOUND	Desired Access: Query Value
6:37:59.0164556 AM	S.exe	4188	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate S
6:37:59.0188185 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate S
6:37:59.0188342 AM	S.exe	4188	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\Reso...	NAME NOT FOUND	Length: 24
6:37:59.0188424 AM	S.exe	4188	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
6:37:59.0191434 AM	S.exe	4188	CreateFile	C:\Windows	SUCCESS	Desired Access: Execute/Traverse, Synchr
6:37:59.0193282 AM	S.exe	4188	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7ffb3e610000, Image Size:
6:37:59.0194178 AM	S.exe	4188	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7ffb3efe0000, Image Size:
6:37:59.0197174 AM	S.exe	4188	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: Read Attributes, Dispositic
6:37:59.0199446 AM	S.exe	4188	CreateFile	C:\Windows	SUCCESS	Desired Access: Read Attributes, Synchron
6:37:59.0199685 AM	S.exe	4188	QueryNameInformatio...	C:\Windows	SUCCESS	Name: \Windows
6:37:59.0199803 AM	S.exe	4188	CloseFile	C:\Windows	SUCCESS	
6:37:59.0200057 AM	S.exe	4188	RegOpenKey	HKLM\Software\Microsoft\Wow64\x86	SUCCESS	Desired Access: Read
6:37:59.0200213 AM	S.exe	4188	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\x86\S.exe	NAME NOT FOUND	Length: 520
6:37:59.0200272 AM	S.exe	4188	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\x86\(Default)	SUCCESS	Type: REG_SZ, Length: 26, Data: wow64cp
6:37:59.0200356 AM	S.exe	4188	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\x86	SUCCESS	
6:37:59.0201208 AM	S.exe	4188	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x778a0000, Image Size: 0x9
6:37:59.0203212 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value
6:37:59.0203325 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
6:37:59.0203586 AM	S.exe	4188	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformationClass: KeySetHandleTa
6:37:59.0203718 AM	S.exe	4188	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\Rais...	NAME NOT FOUND	Length: 80
6:37:59.0203823 AM	S.exe	4188	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
6:37:59.0203992 AM	S.exe	4188	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Se...	REPARSE	Desired Access: Query Value
6:37:59.0204076 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Seg...	NAME NOT FOUND	Desired Access: Query Value
6:37:59.0204536 AM	S.exe	4188	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate S
6:37:59.0204601 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate S
6:37:59.0204676 AM	S.exe	4188	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformationClass: KeySetHandleTa
6:37:59.0204727 AM	S.exe	4188	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\Reso...	NAME NOT FOUND	Length: 24
6:37:59.0204794 AM	S.exe	4188	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
6:37:59.0207599 AM	S.exe	4188	CreateFile	C:\Users\IEUser\Desktop	SUCCESS	Desired Access: Execute/Traverse, Synchr
6:37:59.0208902 AM	S.exe	4188	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76e60000, Image Size: 0xe
6:37:59.0210278 AM	S.exe	4188	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x75c80000, Image Size: 0x1f
6:37:59.0216044 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	REPARSE	Desired Access: Read
6:37:59.0216137 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
6:37:59.0216253 AM	S.exe	4188	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	KeySetInformationClass: KeySetHandleTa
6:37:59.0216314 AM	S.exe	4188	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAp...	NAME NOT FOUND	Length: 548
6:37:59.0216375 AM	S.exe	4188	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUs...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
6:37:59.0216455 AM	S.exe	4188	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
6:37:59.0217608 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Query Value, Set Value
6:37:59.0217689 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, Set Value
6:37:59.0217810 AM	S.exe	4188	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	REPARSE	Desired Access: Read

Showing 5,983 of 274,681 events (2.1%) Backed by virtual memory

איור מס' 9 – תיעוד התהליכים במכונה בעזרת הכלי "ProcMon"

לאחר סינון התהליכים שרצו על גבי המכונה לאחר הפעלת הקובץ ניתן לראות בבירור שהקובץ הוא פעיל מאוד, נוצרים ונסגרים תהליכים, העלאה של קבצים, פעולות שונות ומשונות בספריות המערכת.

כיצד ניתן להימנע מהדבקה של RAT'S?

1. ראשית יש להימנע לחלוטין מפתיחת הודעות דוא"ל ממשתמשים לא מוכרים, דרך נפוצה מאוד היא העברה של הקובץ בתוך הודעת ספאם ולפעמים מספיק רק להוריד את הקובץ בשביל להידבק.
2. הורידו רק תוכנות עם ביקורות חיוביות ממקורות אמינים תוכנות מזויפות הן דרך נוספת בה ניתן להדבק. הקורבן יבחר להתקין תוכנה, בלי להבין שהיא נושאת על גבה טרויאני.
3. המנעו משימוש בכתובות URL מקוצרות וחשבו בזהירות לפני שתאשרו הורדה מכל סוג, כל הורדה היא איום פוטנציאלי.
4. המנעו מלחיצה על באנרים של פרסומות וביקור באתרים לא מוכרים כדי לצמצם את הסיכון. לא תמיד ההדבקה בטרויאני נעשית דרך הורדה אקטיבית. ישנם מקרים בהם ביקור פשוט באתר מודבק מספיק כדי שתדבקו בעצמכם.
5. השתמשו בתוכנות חומת אש – התוכנה מבצעת סריקה של הנתונים המגיעים למכשיר שלכם מהאינטרנט. רוב מערכות ההפעלה מגיעות עם חומת אש מובנית.
6. התקינו אנטי וירוס באיכות גבוהה תוכנות אנטי וירוס ואנטי תוכנות זדוניות הן קו ההגנה הראשון שלכם כך שקריטי שהן יהיו הטובות ביותר שיש. תוכנות אלו יכולות לסרוק את המכשיר שלכם, ולהתריע במידה ואחת נמצאה.