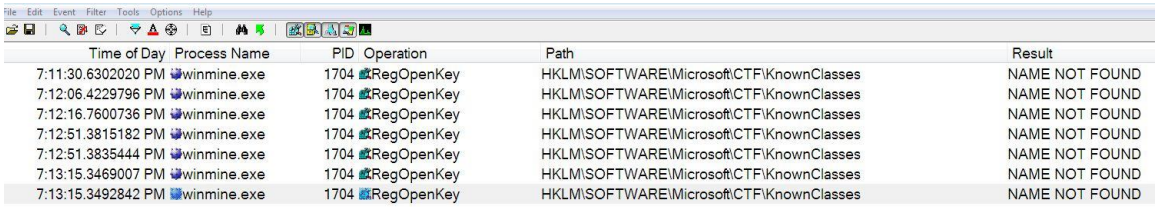
Operating Systems Security Vulnerabilities and Cyber Defenses

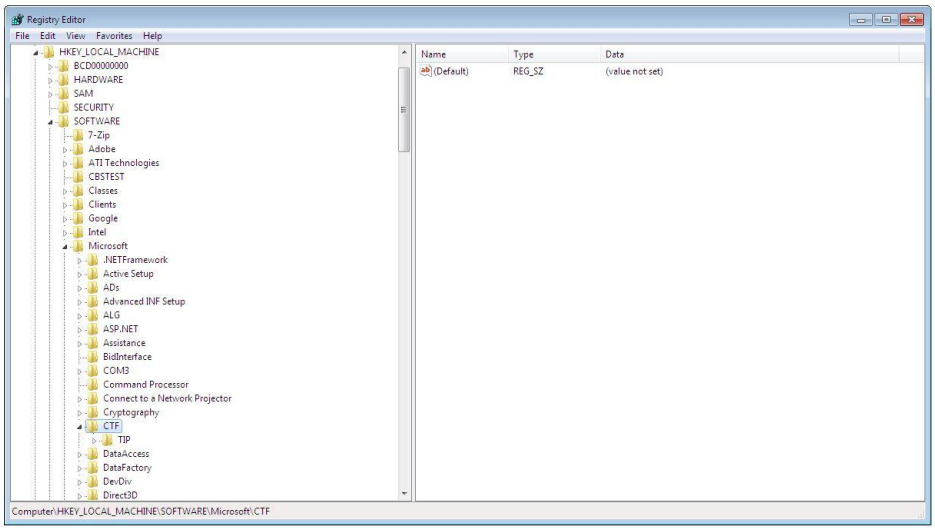
תרגיל 1

חלק א

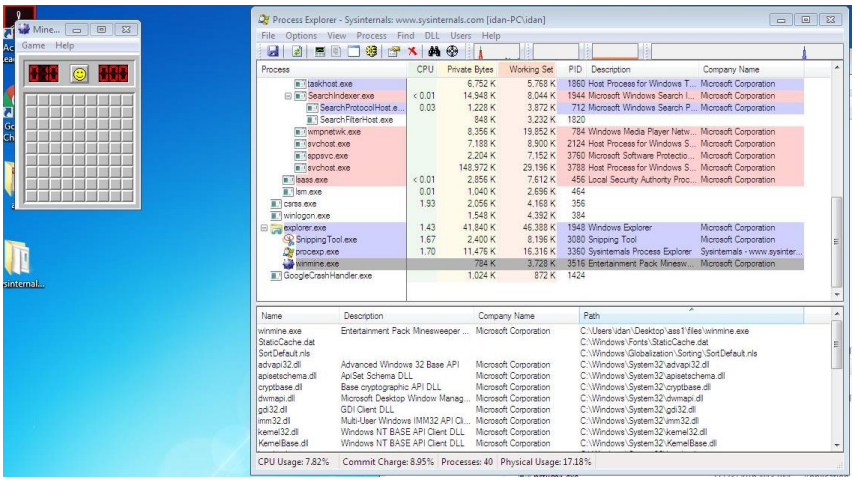
1)נעזרנו ב-regedit כדי לשנות את נתוני טבלת הנצחונות. לשם חיפוש המקום המתאים ב-registry, נעזרנו תחילה ב-process monitor. לחצנו על "include processes from window" ובחרנו בחלון של המשחק שפתחנו. לאחר מכן הופיע תהליך המשחק ב-procmon. לחצנו על reset scores ואז ב-procmon נוספו שני אירועים חדשים הניגשים לערך
HKLM\SOFTWARE\Microsoft\CTF\KnownClasses. כאשר חיפשנו את הנתיב הזה ב-regedit, לא מצאנו את התיקייה KnownClasses תחת CTF.



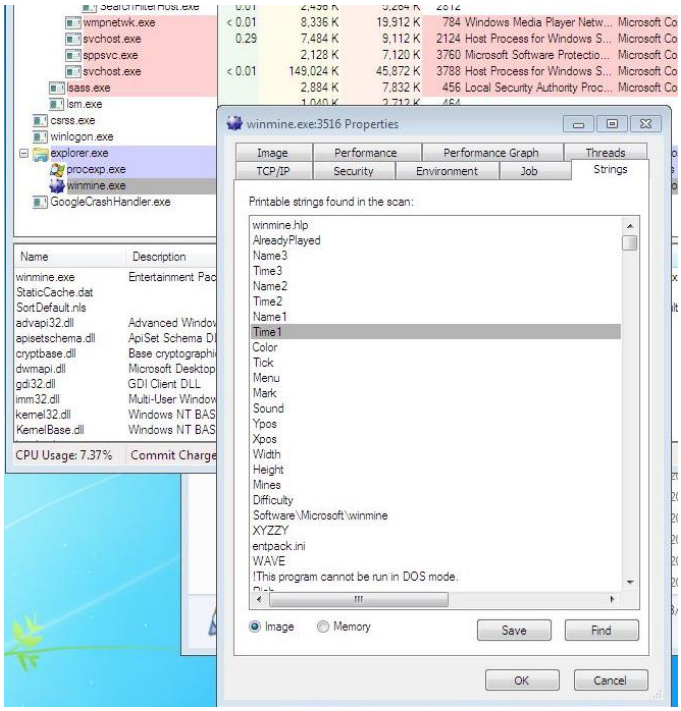
Time of Day	Process Name	PID	Operation	Path	Result
7:11:30.6302020 PM	winmine.exe	1704	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\KnownClasses	NAME NOT FOUND
7:12:06.4229796 PM	winmine.exe	1704	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\KnownClasses	NAME NOT FOUND
7:12:16.7600736 PM	winmine.exe	1704	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\KnownClasses	NAME NOT FOUND
7:12:51.3815182 PM	winmine.exe	1704	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\KnownClasses	NAME NOT FOUND
7:12:51.3835444 PM	winmine.exe	1704	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\KnownClasses	NAME NOT FOUND
7:13:15.3469007 PM	winmine.exe	1704	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\KnownClasses	NAME NOT FOUND
7:13:15.3492842 PM	winmine.exe	1704	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\KnownClasses	NAME NOT FOUND



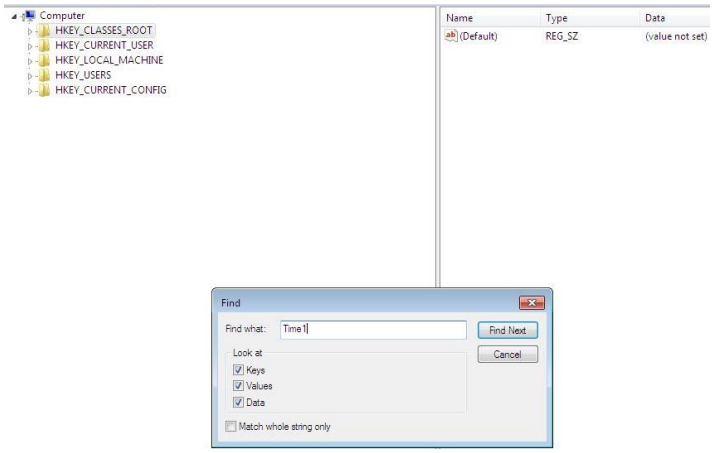
משנכשלנו בדרך זו, החלטנו לנסות את ה-process explorer כדי לחפש מידע נוסף על התהליך.

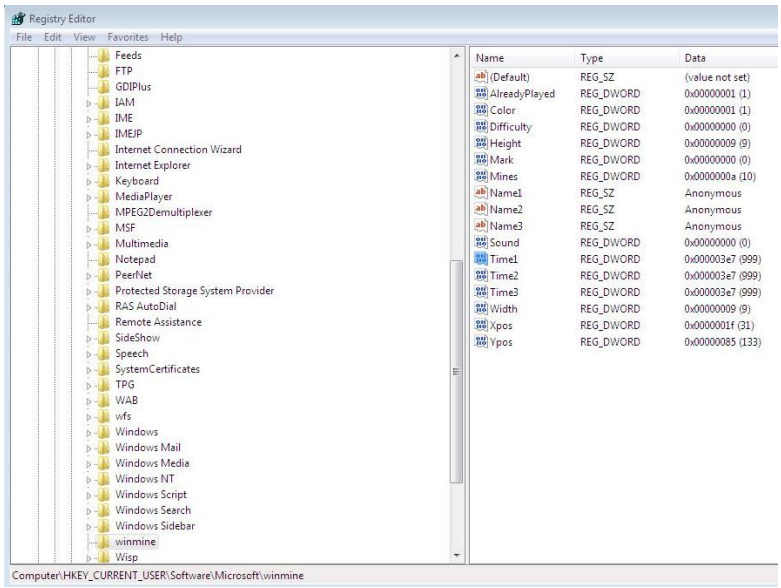


איתרנו את minesweeper (winmine.exe) ב-procexp, ונכנסנו ל-properties של התהליך. שם נכנסנו ללשונית של strings, וראינו strings "חשודים" בשמות Time1, Time2, Time3.

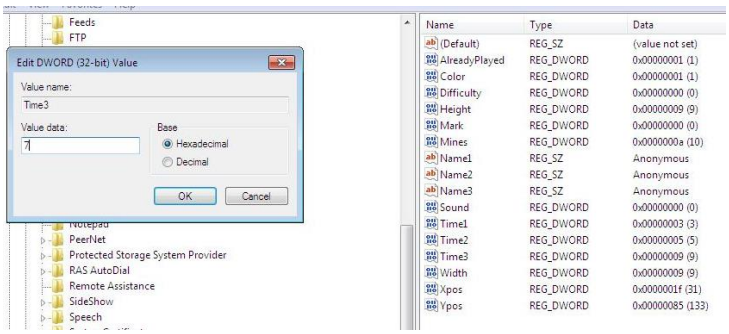


חזרנו ל-regedit וחיפשנו בחיפוש את הסטרינג Time1.

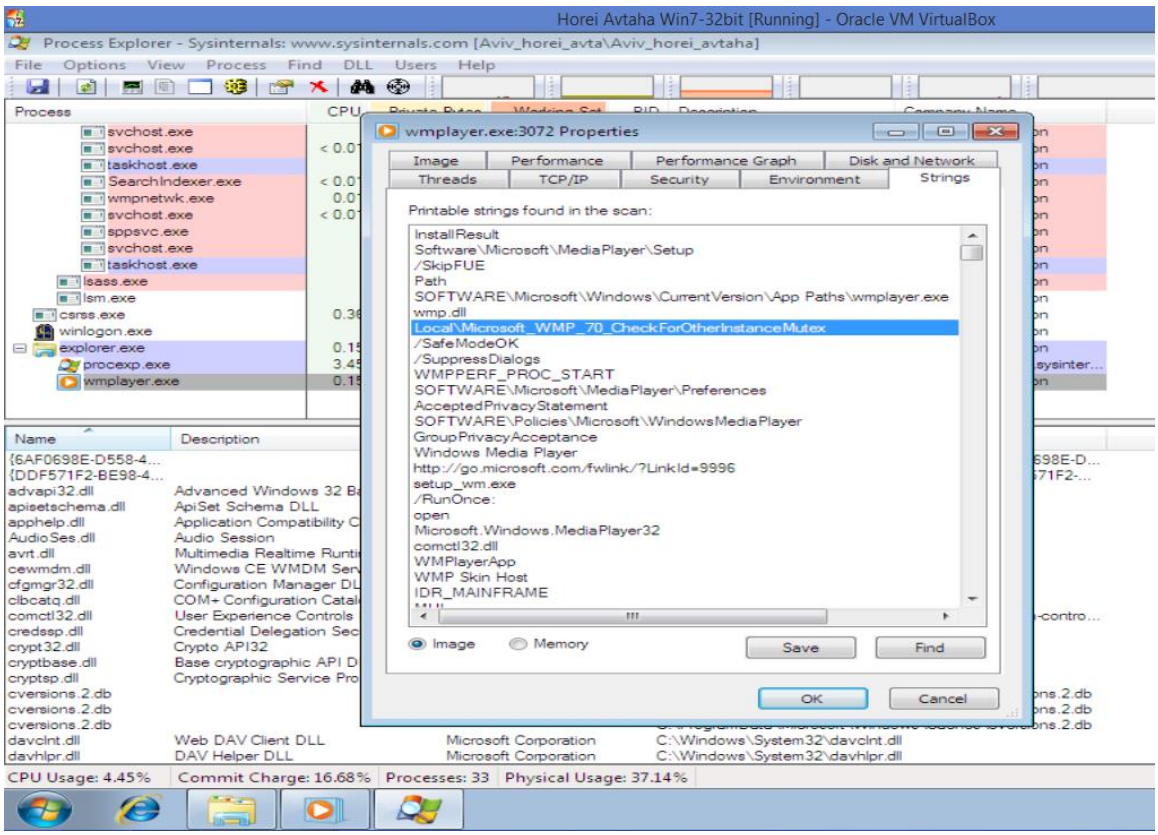




שינינו את הערכים של Time1, Time2, Time3 ל-3,5 ו-7. ולאחר שסגרנו ופתחנו מחדש את המשחק, טבלת ה-best times הציגה את הערכים החדשים.

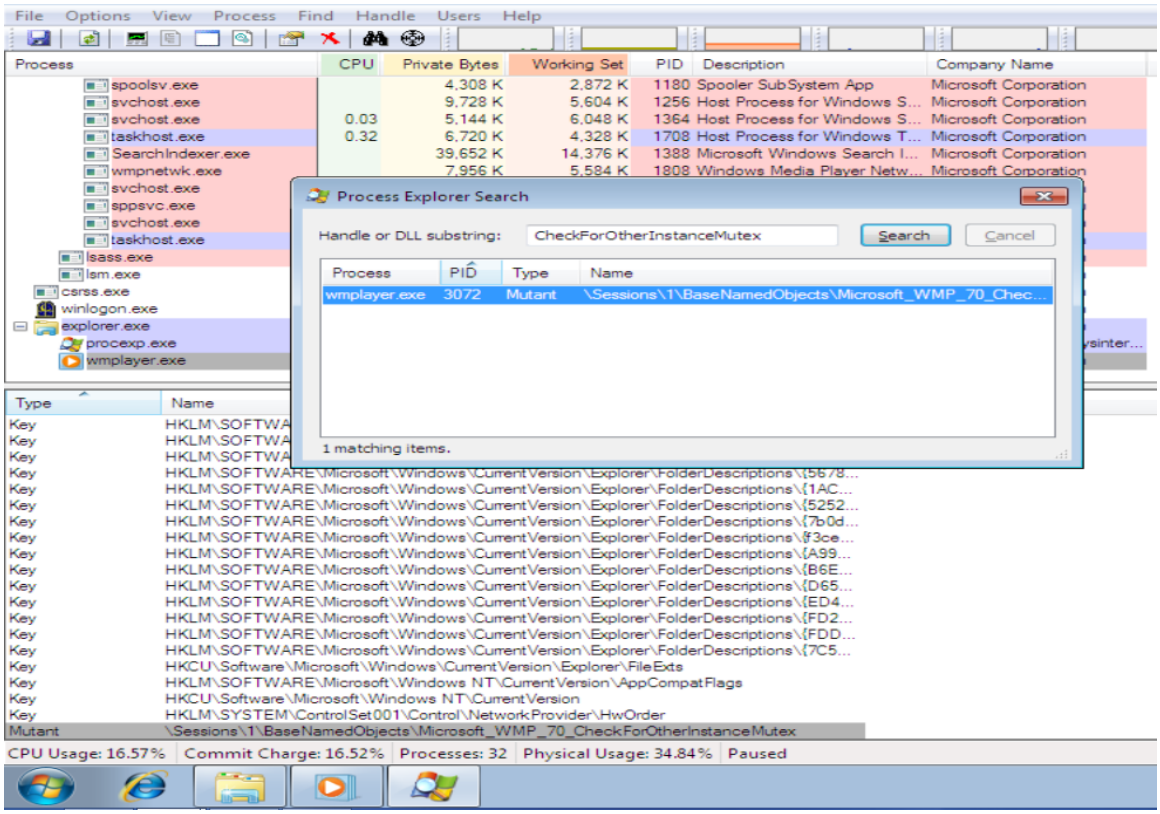


2)הפעלנו את windows media player במקביל ל-process explorer. הפעם, ניגשנו מיד ל-properties של התהליך וללשונית ה-strings. שם מצאנו סטרינג מעניין:
"Local\Microsoft_WMP_70_CheckForOtherInstanceMutex".

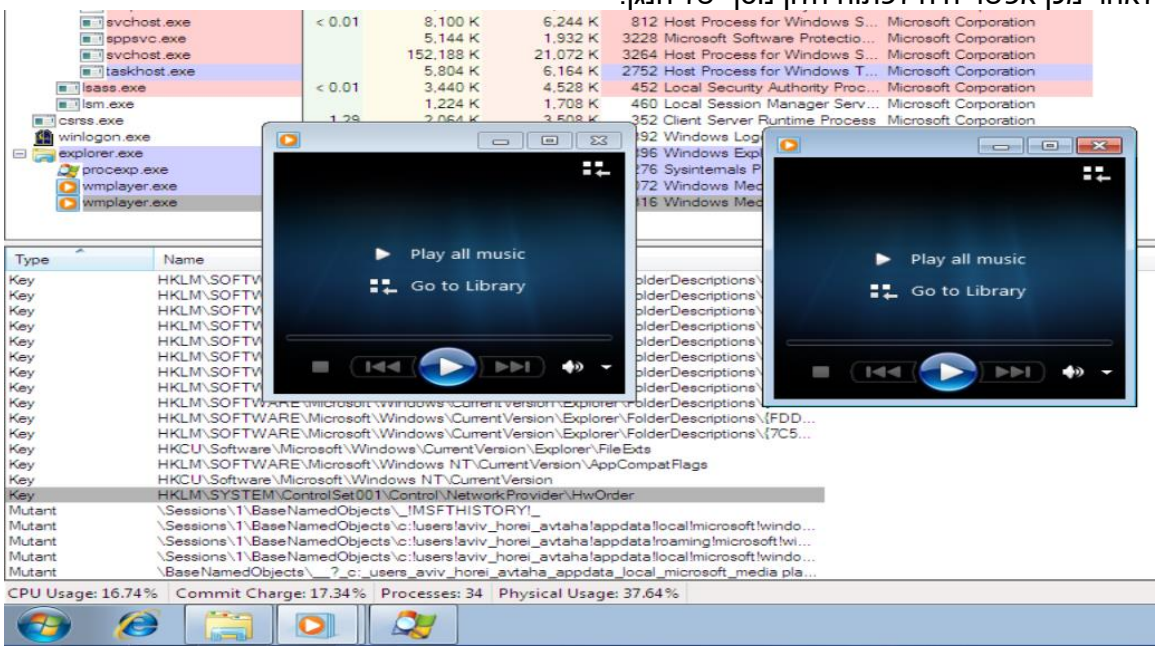


ידענו ש-mutex זה אובייקט מסונכרן, ומהשם היה ברור שמדובר ב-mutex שאחראי למניעת פתיחת חלונות נוספים.

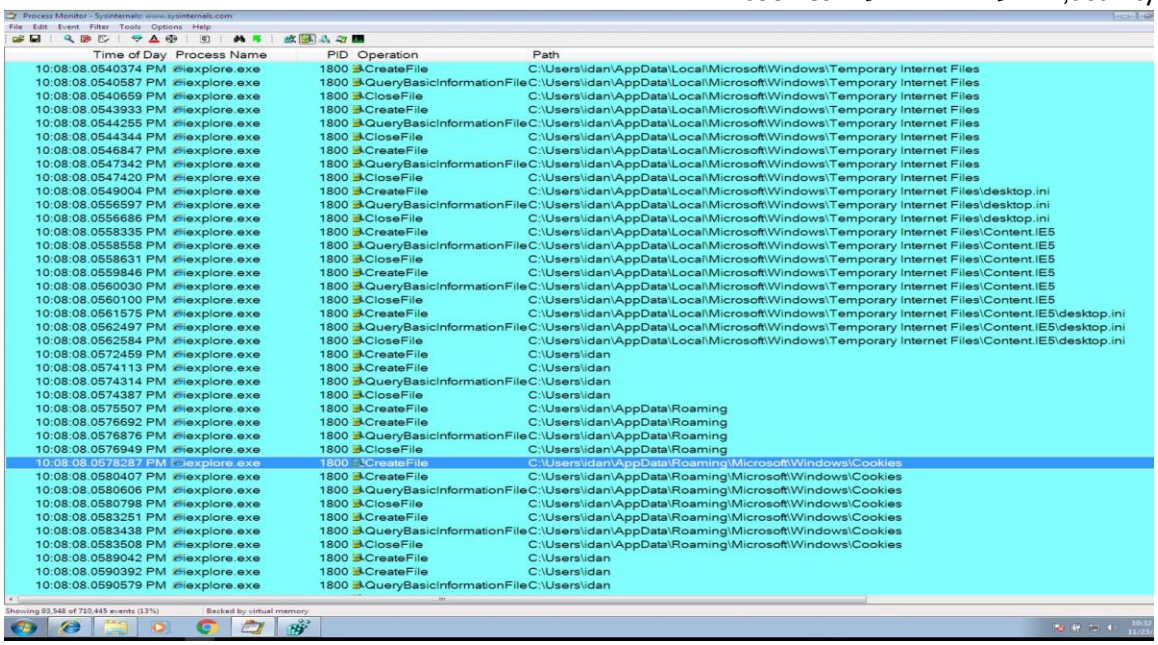
בסרגל הכלים של procexp מצאנו כפתור "view handles". למדנו בכיתה שהמשאבים של מערכת ההפעלה מיוצגים ע"י handles. לחצנו על הכפתור וברשימת ההנדלים חיפשנו "CheckForOtherInstanceMutex".



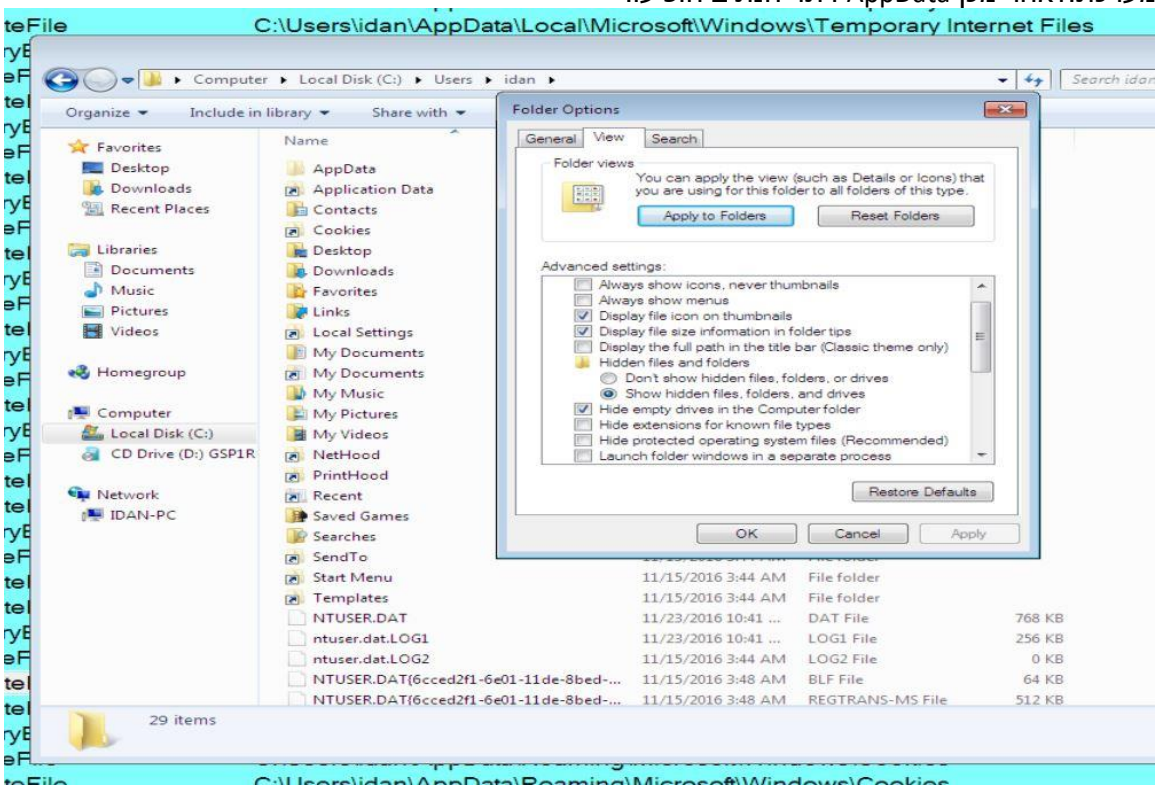
משאיתרנו את ה-mutex, סגרנו אותו (אפשרי רק בהרצה של procexp כאדמיניסטרטור).
לאחר מכן אפשר היה לפתוח חלון נוסף של הנגן.



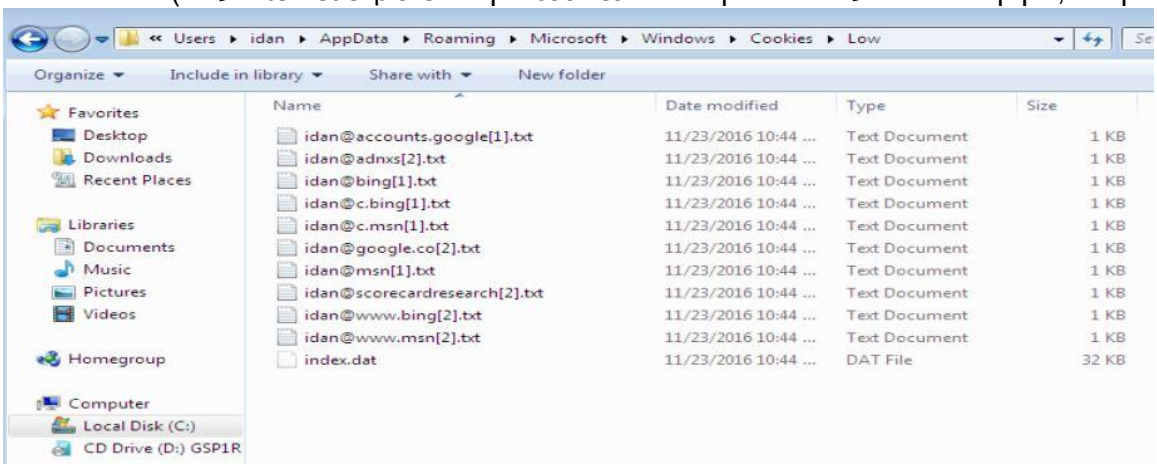
3)פתחנו את ה-internet explorer ונכנסנו ל-process monitor. הגדרנו אותו כך שיראה רק file system activity, והפעלנו חיפוש על "cookies".



מצאנו מספרים אירועים תחת התהליך iexplore.exe (אינטרנט אספלורר) בתיקייה C:\\Users\Idan\AppData\Roaming\Microsoft\Windows\Cookies. כאשר ניסינו לגשת לנתיב זה, לא נראתה התיקייה AppData. שינינו את הגדרות ה-file explorer כך שיציג תיקיות וקבצים נסתרים וקבצי מערכת.לאחר מכן AppData ויתר הנתיב הופיעו.



בתוך cookies הייתה תיקייה נוספת, Low. הסתבר שהיא למעשה ה-cookie jar (זיהינו לפי שמות הקבצים, וכן קבצים אלה נעלמו כשמחקנו את ה-cookies דרך ה-internet explorer עצמו).



חלק ב:

בתחילת ריצתה הנוזקה מנסה לבצע acquire ל Mutex בשם

' Global\\{2384ec59-0df8-4ab9-918c-843740924a28}'. לשם מניעת ריצה כפולה של הנוזקה.

```
PS C:\Users\idan\Desktop\ass1\files> .\trafficconverter.exe m0nk3y | tee out.txt
2016-12-11 18:49:18,170 [3244:INFO] main.main.106: >>>>>>>>>> Initializing monkey (ChaosMonkey): PID 3244 <<<<<<<<<<
2016-12-11 18:49:18,170 [3244:INFO] monkey.initialize.38: Monkey is initializing...
2016-12-11 18:49:18,170 [3244:DEBUG] system_singleton.try_lock.60: Global singleton mutex 'Global\\{2384ec59-0df8-4ab9-918c-843740924a28}' acquired
2016-12-11 18:49:18,170 [3244:INFO] monkey.start.68: Monkey is running...
```

לאח מכן הנוזקה ראשית בודקת קיום חיבור לאינטרנט ע"י שליחת פינג לגוגל ולאחר מכן מנסה להתחבר לשרת C&C (Command&Control - סרבר ששולט בהתנהגות נוזקות) בכתובת 41.50.73.31 בפורט 5000.

```
2016-12-11 18:49:24,398 [3244:DEBUG] control.wakeup.26: Trying to wake up with C&C servers list: ['41.50.73.31:5000']

Pinging www.google.com [216.58.212.228] with 32 bytes of data:
Reply from 216.58.212.228: bytes=32 time=74ms TTL=51

Ping statistics for 216.58.212.228:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 74ms, Maximum = 74ms, Average = 74ms
2016-12-11 18:49:25,160 [3244:DEBUG] control.wakeup.54: Trying to connect to server: 41.50.73.31:5000
2016-12-11 18:49:25,170 [3244:INFO] connectionpool._new_conn.805: Starting new HTTPS connection (1): 41.50.73.31
2016-12-11 18:49:45,177 [3244:WARNING] control.wakeup.65: Error connecting to control server 41.50.73.31:5000: HTTPSConnectionPool(host='41.50.73.31', port=5000): Max retries exceeded with url: /api/monkey (Caused by ConnectTimeout
(Error(<requests.packages.urllib3.connection.VerifiedHTTPSConnection object at 0x0385DF10>, 'Connection to 41.50.73.31 timed out. (connect timeout=20)'))
```

ניתן לראות זאת גם בprocmon

6:49:27.4388043 PM	trafficconverter.e...	3244	TCP Reconnect	idan-PC:49198 -> 41.50.73.31:5000	SUCCESS	Length: 0, seqnum: 0, connid: 0
6:49:33.4374391 PM	trafficconverter.e...	3244	TCP Reconnect	idan-PC:49198 -> 41.50.73.31:5000	SUCCESS	Length: 0, seqnum: 0, connid: 0
6:49:44.4743898 PM	trafficconverter.e...	3244	UDP Send	idan-PC:5007 -> 224.1.1.1:5007	SUCCESS	Length: 1, seqnum: 0, connid: 0
6:49:44.4744231 PM	trafficconverter.e...	3244	UDP Receive	224.1.1.1:5007 -> idan-PC:5007	SUCCESS	Length: 1, seqnum: 0, connid: 0
6:49:54.7340055 PM	trafficconverter.e...	3244	UDP Send	idan-PC:5007 -> 224.1.1.1:5007	SUCCESS	Length: 1, seqnum: 0, connid: 0
6:49:54.7340600 PM	trafficconverter.e...	3244	UDP Receive	224.1.1.1:5007 -> idan-PC:5007	SUCCESS	Length: 1, seqnum: 0, connid: 0
6:50:04.7330900 PM	trafficconverter.e...	3244	UDP Send	idan-PC:5007 -> 224.1.1.1:5007	SUCCESS	Length: 1, seqnum: 0, connid: 0
6:50:04.7331314 PM	trafficconverter.e...	3244	UDP Receive	224.1.1.1:5007 -> idan-PC:5007	SUCCESS	Length: 1, seqnum: 0, connid: 0

הנוזקה גם שולחת multicast לכתובת 224.1.1.1 לשם חיפוש מאזינים אפשריים אך מקבלת תשובה רק מהמחשב הנוכחי (אין מאזינים נוספים פרט אליה).
משהנוזקה לא הצליחה להתחבר לשרת C&C היא מתחילה את פעולתה עם קונפיגורציה דיפלוטיבית.
בשלב זה הנוזקה מוצאת את כתובת הip של מחשב הhost ומתחילה חיפוש רחב בטווח הכתובות של כתובת ה host.

```
2016-12-11 18:49:45,177 [3244:INFO] control.wakeup.69: Starting tunnel lookup...
2016-12-11 18:49:45,207 [3244:INFO] tunnel.find_tunnel.71: Trying to find using adapter 10.0.0.10
2016-12-11 18:49:55,213 [3244:INFO] tunnel.find_tunnel.71: Trying to find using adapter 10.0.0.10
2016-12-11 18:50:05,467 [3244:INFO] tunnel.find_tunnel.71: Trying to find using adapter 10.0.0.10
2016-12-11 18:50:15,471 [3244:INFO] control.wakeup.77: No tunnel found
2016-12-11 18:50:15,471 [3244:DEBUG] monkey.start.88: default server:
2016-12-11 18:50:15,471 [3244:DEBUG] monkey.start.92: Calling system info collection
2016-12-11 18:50:15,502 [3244:DEBUG] monkey.start.102: Running with depth: 2
2016-12-11 18:50:15,522 [3244:INFO] network_scanner.initialize.27: Found local IP addresses of the machine: ['10.0.0.10']
2016-12-11 18:50:15,562 [3244:INFO] network_scanner.initialize.36: Base local networks to scan are: [<FixedRange >, <FixedRange 10.0.0.1,10.0.0.2,10.0.0.3,
0.0.0.13,10.0.0.14,10.0.0.15,10.0.0.16,10.0.0.17,10.0.0.18,10.0.0.19,10.0.0.20,10.0.0.21,10.0.0.22,10.0.0.23,10.0.0.24,10.0.0.25,10.0.0.26,10.0.0.27,10.0.0.
0.0.0.36,10.0.0.37,10.0.0.38,10.0.0.39,10.0.0.40,10.0.0.41,10.0.0.42,10.0.0.43,10.0.0.44,10.0.0.45,10.0.0.46,10.0.0.47,10.0.0.48,10.0.0.49,10.0.0.50,10.0.0
0.0.0.59,10.0.0.60,10.0.0.61,10.0.0.62,10.0.0.63,10.0.0.64,10.0.0.65,10.0.0.66,10.0.0.67,10.0.0.68,10.0.0.69,10.0.0.70,10.0.0.71,10.0.0.72,10.0.0.73,10.0.0
0.0.0.82,10.0.0.83,10.0.0.84,10.0.0.85,10.0.0.86,10.0.0.87,10.0.0.88,10.0.0.89,10.0.0.90,10.0.0.91,10.0.0.92,10.0.0.93,10.0.0.94,10.0.0.95,10.0.0.96,10.0.0
104,10.0.0.105,10.0.0.106,10.0.0.107,10.0.0.108,10.0.0.109,10.0.0.110,10.0.0.111,10.0.0.112,10.0.0.113,10.0.0.114,10.0.0.115,10.0.0.116,10.0.0.117,10.0.0.1
.125,10.0.0.126,10.0.0.127,10.0.0.128,10.0.0.129,10.0.0.130,10.0.0.131,10.0.0.132,10.0.0.133,10.0.0.134,10.0.0.135,10.0.0.136,10.0.0.137,10.0.0.138,10.0.0.1
0.146,10.0.0.147,10.0.0.148,10.0.0.149,10.0.0.150,10.0.0.151,10.0.0.152,10.0.0.153,10.0.0.154,10.0.0.155,10.0.0.156,10.0.0.157,10.0.0.158,10.0.0.159,10.0.0
.0.167,10.0.0.168,10.0.0.169,10.0.0.170,10.0.0.171,10.0.0.172,10.0.0.173,10.0.0.174,10.0.0.175,10.0.0.176,10.0.0.177,10.0.0.178,10.0.0.179,10.0.0.180,10.0.
0.0.188,10.0.0.189,10.0.0.190,10.0.0.191,10.0.0.192,10.0.0.193,10.0.0.194,10.0.0.195,10.0.0.196,10.0.0.197,10.0.0.198,10.0.0.199,10.0.0.200,10.0.0.201,10.0
.0.209,10.0.0.210,10.0.0.211,10.0.0.212,10.0.0.213,10.0.0.214,10.0.0.215,10.0.0.216,10.0.0.217,10.0.0.218,10.0.0.219,10.0.0.220,10.0.0.221,10.0.0.222,10.
0.0.0.230,10.0.0.231,10.0.0.232,10.0.0.233,10.0.0.234,10.0.0.235,10.0.0.236,10.0.0.237,10.0.0.238,10.0.0.239,10.0.0.240,10.0.0.241,10.0.0.242,10.0.0.243,10
10.0.0.251,10.0.0.252,10.0.0.253,10.0.0.254>]
2016-12-11 18:50:15,562 [3244:DEBUG] network_scanner.get_victim_machines.45: Scanning for potential victims in the network <FixedRange >
2016-12-11 18:50:15,562 [3244:DEBUG] network_scanner.get_victim_machines.45: Scanning for potential victims in the network <FixedRange 10.0.0.1,10.0.0.2,10
.0.12,10.0.0.13,10.0.0.14,10.0.0.15,10.0.0.16,10.0.0.17,10.0.0.18,10.0.0.19,10.0.0.20,10.0.0.21,10.0.0.22,10.0.0.23,10.0.0.24,10.0.0.25,10.0.0.26,10.0.0.27
0.35,10.0.0.36,10.0.0.37,10.0.0.38,10.0.0.39,10.0.0.40,10.0.0.41,10.0.0.42,10.0.0.43,10.0.0.44,10.0.0.45,10.0.0.46,10.0.0.47,10.0.0.48,10.0.0.49,10.0.0.50
.0.58,10.0.0.59,10.0.0.60,10.0.0.61,10.0.0.62,10.0.0.63,10.0.0.64,10.0.0.65,10.0.0.66,10.0.0.67,10.0.0.68,10.0.0.69,10.0.0.70,10.0.0.71,10.0.0.72,10.0.0.73
.0.81,10.0.0.82,10.0.0.83,10.0.0.84,10.0.0.85,10.0.0.86,10.0.0.87,10.0.0.88,10.0.0.89,10.0.0.90,10.0.0.91,10.0.0.92,10.0.0.93,10.0.0.94,10.0.0.95,10.0.0.96
10.0.0.104,10.0.0.105,10.0.0.106,10.0.0.107,10.0.0.108,10.0.0.109,10.0.0.110,10.0.0.111,10.0.0.112,10.0.0.113,10.0.0.114,10.0.0.115,10.0.0.116,10.0.0.117,1
,10.0.0.125,10.0.0.126,10.0.0.127,10.0.0.128,10.0.0.129,10.0.0.130,10.0.0.131,10.0.0.132,10.0.0.133,10.0.0.134,10.0.0.135,10.0.0.136,10.0.0.137,10.0.0.138,
5,10.0.0.146,10.0.0.147,10.0.0.148,10.0.0.149,10.0.0.150,10.0.0.151,10.0.0.152,10.0.0.153,10.0.0.154,10.0.0.155,10.0.0.156,10.0.0.157,10.0.0.158,10.0.0.159
66,10.0.0.167,10.0.0.168,10.0.0.169,10.0.0.170,10.0.0.171,10.0.0.172,10.0.0.173,10.0.0.174,10.0.0.175,10.0.0.176,10.0.0.177,10.0.0.178,10.0.0.179,10.0.0.18
187,10.0.0.188,10.0.0.189,10.0.0.190,10.0.0.191,10.0.0.192,10.0.0.193,10.0.0.194,10.0.0.195,10.0.0.196,10.0.0.197,10.0.0.198,10.0.0.199,10.0.0.200,10.0.0.2
.208,10.0.0.209,10.0.0.210,10.0.0.211,10.0.0.212,10.0.0.213,10.0.0.214,10.0.0.215,10.0.0.216,10.0.0.217,10.0.0.218,10.0.0.219,10.0.0.220,10.0.0.221,10.0.0.
0.229,10.0.0.230,10.0.0.231,10.0.0.232,10.0.0.233,10.0.0.234,10.0.0.235,10.0.0.236,10.0.0.237,10.0.0.238,10.0.0.239,10.0.0.240,10.0.0.241,10.0.0.242,10.0.0
0.250,10.0.0.251,10.0.0.252,10.0.0.253,10.0.0.254>
```

לכל כתובת בטווח הנוזקה מנסה להתחבר בפורטים 22, 222, 445, 135, 3389, 80, 8080, 443, 8008 ולאחר מכן מעדכנת את קובץ הלוג שנמצא ב- C:\Users\idan\AppData\Local\Temp\~df1563.tmp

6:52:10.2532953 PM	trafficconverter.e...	3244	WriteFile	C:\Users\idan\AppData\Local\Temp\~df1563.tmp
6:52:13.2572094 PM	trafficconverter.e...	3244	TCP Reconnect	idan-PC:49239 -> 10.0.0.46:2222
6:52:16.4566270 PM	trafficconverter.e...	3244	TCP Reconnect	idan-PC:49240 -> 10.0.0.46:http
6:52:19.6564144 PM	trafficconverter.e...	3244	TCP Reconnect	idan-PC:49241 -> 10.0.0.46:ssh
6:52:39.1047278 PM	trafficconverter.e...	3244	QueryStandardInformationFile	C:\Users\idan\AppData\Local\Temp\~df1563.tmp
6:52:39.1047535 PM	trafficconverter.e...	3244	QueryStandardInformationFile	C:\Users\idan\AppData\Local\Temp\~df1563.tmp
6:52:39.1047633 PM	trafficconverter.e...	3244	WriteFile	C:\Users\idan\AppData\Local\Temp\~df1563.tmp
6:53:07.9500559 PM	trafficconverter.e...	3244	QueryStandardInformationFile	C:\Users\idan\AppData\Local\Temp\~df1563.tmp
6:53:07.9500807 PM	trafficconverter.e...	3244	QueryStandardInformationFile	C:\Users\idan\AppData\Local\Temp\~df1563.tmp
6:53:07.9500902 PM	trafficconverter.e...	3244	WriteFile	C:\Users\idan\AppData\Local\Temp\~df1563.tmp
6:53:20.5639870 PM	trafficconverter.e...	3244	TCP Reconnect	idan-PC:49260 -> 10.0.0.13:ms-wbt-server
6:53:23.7686177 PM	trafficconverter.e...	3244	TCP Reconnect	idan-PC:49261 -> 10.0.0.13:microsoft-ds
6:53:30.1677958 PM	trafficconverter.e...	3244	TCP Reconnect	idan-PC:49264 -> 10.0.0.13:http

כאשר הנוזקה מגיעה לכתובת בה יש מחשב ברשת היא מנסה להתחבר בעזרת כל אחד מהפרוטוקולים המוגדרים לה ובעזרת מספר סיסמאות בסיסיות כגון '12345678' , 'password' , '1234' , 'Password1!' , 'password'. ניתן לראות זאת בקובץ הלוג(כאן רואים ניסיון גישה ע"י SSH).

```
16:06,213 [3244:INFO] connectionpool._new_conn.805: Starting new HTTPS connection (1): 10.0.0.4
16:07,213 [3244:INFO] connectionpool._new_conn.214: Starting new HTTP connection (1): 10.0.0.4
16:08,216 [3244:INFO] connectionpool._new_conn.805: Starting new HTTPS connection (1): 10.0.0.4
16:09,217 [3244:INFO] connectionpool._new_conn.214: Starting new HTTP connection (1): 10.0.0.4
16:10,219 [3244:INFO] connectionpool._new_conn.805: Starting new HTTPS connection (1): 10.0.0.4
16:11,220 [3244:INFO] connectionpool._new_conn.214: Starting new HTTP connection (1): 10.0.0.4
16:12,220 [3244:INFO] connectionpool._new_conn.805: Starting new HTTPS connection (1): 10.0.0.4
16:13,223 [3244:INFO] connectionpool._new_conn.214: Starting new HTTP connection (1): 10.0.0.4
16:34,233 [3244:INFO] monkey.start.157: Skipping exploiter SmbExploiter host:<VictimHost 10.0.0.4>, os is not supported
16:34,233 [3244:INFO] monkey.start.157: Skipping exploiter WmiExploiter host:<VictimHost 10.0.0.4>, os is not supported
16:44,236 [3244:INFO] monkey.start.157: Skipping exploiter Ms08_067_Exploiter host:<VictimHost 10.0.0.4>, os is not supported
16:44,236 [3244:INFO] monkey.start.160: Trying to exploit <VictimHost 10.0.0.4> with exploiter SSHExploiter...
16:44,256 [3244:DEBUG] transport._log.1563: starting thread (client mode): 0x38b3c70L
16:44,256 [3244:DEBUG] transport._log.1563: Local version/idstring: SSH-2.0-paramiko_2.0.2
16:44,256 [3244:DEBUG] transport._log.1563: Remote version/idstring: SSH-2.0-MS_1.100
16:44,266 [3244:INFO] transport._log.1563: Connected (version 2.0, client MS_1.100)
16:44,298 [3244:DEBUG] transport._log.1563: kex algos:[u'ecdh-sha2-nistp256', u'ecdh-sha2-nistp384', u'ecdh-sha2-nistp521', u'diffie-hellman-group-exchange-s
16:44,298 [3244:DEBUG] transport._log.1563: Kex agreed: diffie-hellman-group14-sha1
16:44,308 [3244:DEBUG] transport._log.1563: Cipher agreed: aes128-ctr
16:44,308 [3244:DEBUG] transport._log.1563: MAC agreed: hmac-sha2-256
16:44,318 [3244:DEBUG] transport._log.1563: Compression agreed: none
16:44,558 [3244:DEBUG] transport._log.1563: kex engine KexGroup14 specified hash_algo <built-in function openssl_sha1>
16:44,558 [3244:DEBUG] transport._log.1563: Switch to new keys ...
16:44,578 [3244:DEBUG] transport._log.1563: userauth is OK
16:44,578 [3244:INFO] transport._log.1563: Authentication (password) failed.
16:44,588 [3244:DEBUG] sshexec.exploit_host.75: Error logging into victim <VictimHost 10.0.0.4> with user root and password 'Password1!': (Authentication fai
16:44,618 [3244:DEBUG] transport._log.1563: starting thread (client mode): 0x38c06d0L
16:44,618 [3244:DEBUG] transport._log.1563: Local version/idstring: SSH-2.0-paramiko_2.0.2
16:44,618 [3244:DEBUG] transport._log.1563: Remote version/idstring: SSH-2.0-MS_1.100
16:44,618 [3244:INFO] transport._log.1563: Connected (version 2.0, client MS_1.100)
16:44,657 [3244:DEBUG] transport._log.1563: kex algos:[u'ecdh-sha2-nistp256', u'ecdh-sha2-nistp384', u'ecdh-sha2-nistp521', u'diffie-hellman-group-exchange-s
16:44,667 [3244:DEBUG] transport._log.1563: Kex agreed: diffie-hellman-group14-sha1
```

כיוון שלא מוגדר באף אחד מהמחשבים ברשת המשתמש root עם אחת מהסיסמאות הנ"ל הנוזקה לא הצליחה להתחבר ולהפיץ את עצמה.

ניתן להסיק כי נוזקה זו נכתבה בשפת python זאת כיוון שהיא יוצרת ומשתמש בקבצים עם הסיומות py, pyw, pyc , pyd שהן סיומות המתאימות לקבצים שנכתבו בשפה זו. ניתן גם לראות ב-Procmon שהנוזקה ניגשת לערכי registry ו dllים של python.

6:49:17.3921925 PM	trafficconverter.e...	3244 ReadFile	C:\Users\idan\Desktop\ass1\files\trafficconverter.exe	SUCCESS	Offset: 13,959,168, Length: 4,096, I/O Flags: N...
6:49:17.3925412 PM	trafficconverter.e...	3244 CloseFile	C:\Users\idan\Desktop\ass1\files\trafficconverter.exe	SUCCESS	
6:49:17.3928496 PM	trafficconverter.e...	3244 CreateFile	C:\Users\idan\AppData\Local\Temp_MEI8282\simplejson	NAME NOT F...	Desired Access: Read Attributes, Disposition: ...
6:49:17.3929247 PM	trafficconverter.e...	3244 CreateFile	C:\Users\idan\AppData\Local\Temp_MEI8282\simplejson.pyd	NAME NOT F...	Desired Access: Generic Read, Disposition: O...
6:49:17.3929977 PM	trafficconverter.e...	3244 CreateFile	C:\Users\idan\AppData\Local\Temp_MEI8282\simplejson.py	NAME NOT F...	Desired Access: Generic Read, Disposition: O...
6:49:17.3930683 PM	trafficconverter.e...	3244 CreateFile	C:\Users\idan\AppData\Local\Temp_MEI8282\simplejson.pyw	NAME NOT F...	Desired Access: Generic Read, Disposition: O...
6:49:17.3931544 PM	trafficconverter.e...	3244 CreateFile	C:\Users\idan\AppData\Local\Temp_MEI8282\simplejson.pyc	NAME NOT F...	Desired Access: Generic Read, Disposition: O...
6:49:17.3933290 PM	trafficconverter.e...	3244 CreateFile	C:\Users\idan\Desktop\ass1\files\trafficconverter.exe	SUCCESS	Desired Access: Generic Read, Disposition: O...
6:49:17.3933552 PM	trafficconverter.e...	3244 QueryInformationVolume	C:\Users\idan\Desktop\ass1\files\trafficconverter.exe	SUCCESS	VolumeCreationTime: 11/15/2016 11:34:59 PM...
6:49:17.3933650 PM	trafficconverter.e...	3244 QueryAllInformationFile	C:\Users\idan\Desktop\ass1\files\trafficconverter.exe	BUFFER OVE...	CreationTime: 12/6/2016 1:45:50 AM, LastAcc...

6:49:15.5069113 PM	trafficconverter.e...	3244 ReadFile	C:\Users\idan\Desktop\ass1\files\trafficconverter.exe
6:49:15.5069278 PM	trafficconverter.e...	3244 ReadFile	C:\Users\idan\Desktop\ass1\files\trafficconverter.exe
6:49:15.5074035 PM	trafficconverter.e...	3244 ReadFile	C:\Users\idan\Desktop\ass1\files\trafficconverter.exe
6:49:15.5074234 PM	trafficconverter.e...	3244 ReadFile	C:\Users\idan\Desktop\ass1\files\trafficconverter.exe
6:49:15.5080271 PM	trafficconverter.e...	3244 CloseFile	C:\Users\idan\Desktop\ass1\files\trafficconverter.exe
6:49:15.5080765 PM	trafficconverter.e...	3244 RegOpenKey	HKCU\Software\Python\PythonCore\2.7\Modules\pyimod00_crypto_key
6:49:15.5080899 PM	trafficconverter.e...	3244 RegOpenKey	HKLM\Software\Python\PythonCore\2.7\Modules\pyimod00_crypto_key
6:49:15.5081961 PM	trafficconverter.e...	3244 CreateFile	C:\Users\idan\AppData\Local\Temp
6:49:15.5082168 PM	trafficconverter.e...	3244 QueryDirectory	C:\Users\idan\AppData\Local\Temp_MEI8282
6:49:15.5082383 PM	trafficconverter.e...	3244 CloseFile	C:\Users\idan\AppData\Local\Temp

כל הפרטים הנ"ל ניתן גם לראות בקובץ הקונפיגורציה שהנוזקה טוענת ובקובץ הלוג המצורפים בהגשה.

<u>משמעות שרת ה-C&C</u>: ה-IP שהנוזקה מנסה להתחבר אליו הוא של החברה GuardiCore, שיצרה את הנוזקה. שם הנוזקה המקורי הוא Infection Monkey, והיא נועדה לעזור לזהות חורי אבטחה ברשתות מחשבים, ע"פ האתר שלה. אם היא מצליחה להתחבר למכשיר אחר, זה אומר שיש פרצת אבטחה שיש לתקן. באתר מוצגת דוגמא לגרף התפשטות של הנוזקה ברשת לא מאובטחת שהיא הופעלה בה, ומצויין ששרת ה-C&C הוא שיצר את הגרף הזה. כלומר - הנוזקה מתחברת אל השרת הזה כדי שבסיום פעולתה ניתן יהיה לראות תיאור גרפי של ההתפשטות שלה ברשת המחשבים שהיא הופעלה בה.

GuardiCore

PRODUCT PARTNERS COMPANY RESOURCES BLOG SUPPORT

What is the Infection Monkey?

The Infection Monkey is a cyber security testing tool, capable of wandering around the deepest parts of the data center. It will spin up an infected virtual machine inside random parts of your data center, to test for potential security failures. It behaves more like a random hacker than a vulnerability scanner. The Monkey attempts to move around the data center by leveraging different lateral movement methods typical of a real attacker who has already compromised an internal system. When it successfully reaches another machine, it means that there's a security failure that should be fixed.

The Infection Monkey's high level operation is simple. It is designed to scan the network, check for open ports and fingerprint machines using multiple network protocols. After detecting accessible machines, it attempts to attack every single machine using a variety of methods including intelligent password guessing and basic exploits. Infection Monkey is a work in progress and we have ways to go to fully realize its benefits.

The Monkey's actions are designed to be completely safe for use in a production network. The amount of network traffic generated is very small and all the exploits used were written to prevent any damage to the target or attacker. After all, you do not really want to take your data center down. Do you?