



כותב עורך ומגיש: ישראל אקוקה | [LinkedIn](#)

עבודת גמר בנושא: מחקר זיכרון פורנזי ב RAM בכלי Volatility.
הקדמה על הנושא: המחשב שלנו בנוי בצורה שכזאת שכל התוכנות שאנו רואים בעיין על המסך הם תוכנות שרצות על כרטיס הזיכרון RAM ולא על כונן הקשיח שלנו כפי שנוטים לחשוב.
למה אנחנו רוצים לחקור את הזיכרון?
 אנו נלמד ונראה שיש פעמים שתקיפות מתוחכמות רצות ישיר לזיכרון ה RAM ולא משאירות ראיה על הכונן הקשיח ובקבצים והם נטענים ופועלים ישירות לזיכרון ה RAM ולכן זיכרון ה RAM יכול להוות מקום חזק למחקר.

צריך להבין שדפוס פעולה זה הוא מתוחכם היות ולא נשאר ראיה פורנזית ממשית לפעולת התקיפה על המחשב, כל פעם שהמחשב ידלק מחדש או יכבו אותו כל התקיפה והנתיב שלה במערכת והמערכת ההפעלה שרצה ב RAM תמחק! משום שכך בנוי הטכנולוגיה של ה RAM.

אם כן מהו מחקר זיכרון?

המטרה של חקירה כזאת זה לתפוס מידע ש רץ בזיכרון ה RAM של המחשב במצב אונליין שהזיכרון עדין חי על הכרטיס RAM , כך מתנהל בשלושה שלבים המחקר-

• **אנחנו מחליטים לחקור את הזיכרון: Acquire**

- לתפוס תמונת זיכרון. Capture Raw Memory.
- או קובץ של מצב שינה. [Hibernation File](#).

• **אנחנו מוצאים ממצאים בזיכרון: Context**

- למצוא את ה ארטיפקט בזיכרון שלנו. Establish Context.
- חיפוש היסטרים של זיכרון מפתח. Find Key Memory Offsets.

• **לנתח את האלמנטים שהוצאו: Analyze**

- לנתח את הנתונים שהוצאו משלב הקונטקסט. Analyze Data For Significant Elements.
- או שנצליח לשחזר את האלמנטים שלנו. Recover Evidence.



למה אנחנו בהכרח צריכים לחקור את הזיכרון ?

כפי שראינו למעלה הכל מגיע לזיכרון ה RAM ועולה אליו,

כל דבר במערכת ההפעלה חוצה זיכרון RAM:

- תהליכים, DLL's, הליכי משנה.
- תוכנות זדוניות (כולל טכנולוגיות rootkit).
- רכיבי Socket של רשת, כתובות URL, כתובות IP.
- מפתחות רישום ויומני אירועים של Windows.
- ועוד הרבה חפצי זיכרון שנמצא בזיכרון בהמשך ע"י פלאגים ב volatility.

ולפעמים זה אחד המקומות החזקים שלנו לדלות מידע!

היתרונות בניתוח זיכרון!

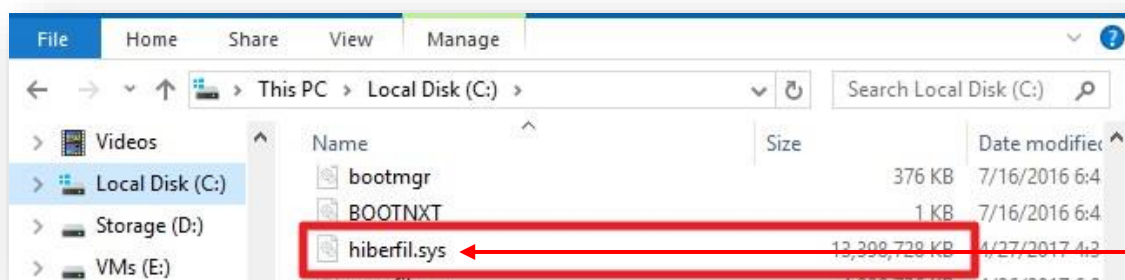
- ההבנה שכל מה שנמצא בזיכרון הוא רץ, לכן אם יש malware שאני רוצה לחקור אותו ואני לא מכיר אותו אני אתן לו לרוץ בתחנת מעבדה ואוכל לעקוב אחריו ולהבין את צעדיו וכך לחקור טוב יותר היות ו...
- הרבה פעמים קשה להבין בצורה יבשה את הפעילות של ה malware בגלל שהם קבצים ארוזים, מוצפנים, מסועפים בינארית, rootkits (כולל מצב ליבה) וכלי הסתרה אחרים ולכן אנחנו בוחרים להריץ אותם על תחנה ולראות איך הם נפרשים על הזיכרון ומכך להבין אותם טוב יותר.
- לאסוף ראיות שלא ניתן למצוא בשום מקום אחר על דיסק היות ויש malware שהם מתוחכמים והם רצים רק על הזיכרון RAM שלנו ולא משאירים ראיה על הדיסק קשיח.
- ומחקר טוב שלנו יוכל למצוא תוכנות זדוניות שהם על הזיכרון בלבד.

ההבדלים בין המצבים - Hibernation Vs Sleep

• בהתאם לגירסה המחשב (קיים במחשבים ניידים) קיימות מספר אפשרויות לחיסכון בצריכת חשמל ב Windows כאשר המחשב אינו בשימוש.

Sleep משתמש בשיטה שהמחשב עולה מהר יותר וכך הוא שומר על המידע בזיכרון ה RAM של המחשב, מתאים למצב שאתה ההולך וחוזר עוד מעט.

• **Hibernation** חוסך עוד יותר כוח על-ידי שמירת זיכרון ה RAM שעכשיו רץ במחשב לתוך קובץ מיוחד אל הכונן הקשיח, כך הוא מכבה את כל ה service's והמערכת כולה ויוצר מצב שהמחשב לא פועל והסוללה לא נגמרת- וכך נשמר הסוללה יותר, מתאים למצב שאתה הולך לזמן ארוך מהמחשב.



ניתן לקרוא ברחבה להבנה עמוקה יותר, חשוב להבנת המחקר!

Windows מספק מספר אפשרויות לחיסכון בצריכת חשמל כאשר אינך משתמש בהתקן שלך, ומסייע לייעל אותו ככל האפשר. אפשרויות אלה הולכות להיות שימושיות ביותר כאשר אתה משתמש במחשב נייד, עוזר לחסוך חיי הסוללה כך שזה נמשך כל היום, אבל גם שימושי כדי לדעת אם אתה רוצה לעשות את החלק שלך עבור הסביבה.

נסביר את ההבדלים בין מצב שינה למצב שינה, מה המחשב שלך עושה כאשר הוא פועל למטה ומתי עליך להשתמש במצב שינה אחד על השני.

מצב שינה
מצב שינה דומה למצב המתנה של הטלוויזיה. כאשר המחשב נכנס למצב שינה כל התהליכים שלו מופסקים והפעולות מופסקות, כאשר כל התוכניות, היישומים והמסמכים הפתוחים מאוחסנים ב- RAM של המערכת.

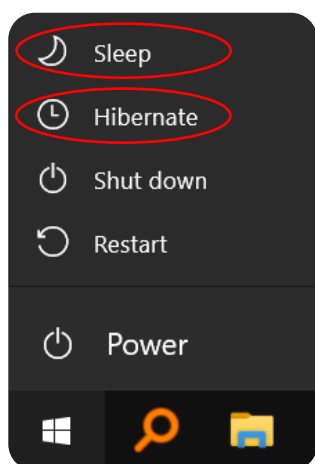
המחשב טכנית נשאר על ידי שימוש קצת כוח, לרוב שהוא מוכן לקפוץ בחזרה לפעולה בהתראה של רגעים - זה צריך לקחת רק כמה שניות עבור המחשב שלך לחדש את התפקוד הרגיל לאחר שינה. מצב שינה הוא נהדר אם אתה הולך לעזוב את המחשב שלך לתקופה קצרה של זמן. אם אתה רוצה להיות יעיל ככל האפשר עם הכוח שלך אתה יכול להגדיר את המחשב שלך ללכת לישון לאחר תקופה של חוסר פעילות [באפשרויות צריכת החשמל שלך](#).

מצב שינה

מצב שינה דומה למדי למצב שינה אך עם כמה הבדלים מרכזיים חשובים.

כאשר המחשב נכנס למצב מצב (Hibernation מצב שינה), היישומים והמסמכים הפתוחים נשמרים בדיסק הקשיח של המחשב ולא ב- RAM שלו. הבדל זה מאפשר למחשב לכבות באופן יעיל לחלוטין, מה שאומר שהוא לא ישתמש בחשמל כלל.

ברגע שתעיר אותו ממצב Hibernation הכל יהיה בדיוק איפה שהשאר אתה, אבל זה ייקח את המחשב שלך יותר זמן להתעורר מאשר ממצב שינה כפי שהוא יצטרך לאחר מידע מהדיסק הקשיח ולא RAM. זה יכול להיעשות הרבה יותר מהר אם אתה משתמש [בכונן מצב מוצק](#) ולא בכונן קשיח רגיל.





Memory Forensics - Volatility








מה הוא Volatility ?

- Volatility - יכול לעבד קבצי Dump של RAM במספר תבניות שונות.
- משמש לעיבוד קבצי Dump של קריסה, קבצי עמודים וקבצי מצב שינה.
- יש תוספים שימושיים רבים שהופכים אותו לכלי חזק מאוד שמתווספות עם הזמן.

הגדרה והתקנת Volatility – LINUX & Windows

- ב-Windows אנו יכולים [להוריד כאן בקישור](#).
- ב-Linux נוריד אותו מ-Github.
- [git clone](#)
- <https://github.com/volatilityfoundation/volatility>
- כדי להתקין נפעיל את הפקודות:
 - `python setup.py install`
 - כדי לבדוק את Volatility אנו מפעילים אותו בפקודה `python vol.py -h` הבאה

כך זה נראה הקובץ בתיקייה בשולחן העבודה,

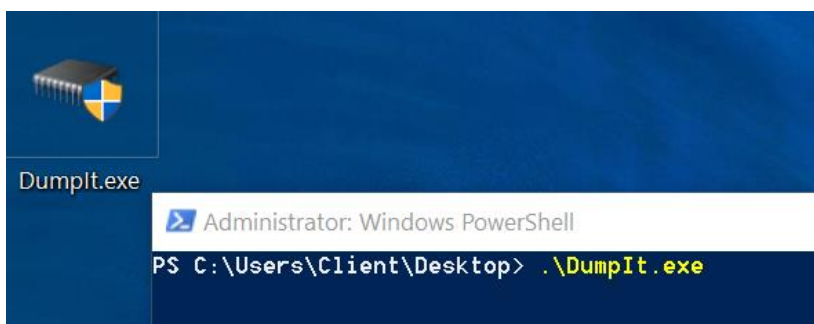
	AUTHORS.txt	27/12/2016 17:44	Text Document	1 KB
	CREDITS.txt	27/12/2016 17:52	Text Document	4 KB
	Lab Exercise.vmva	16/05/2021 09:08	VMVA File	524,288 KB
	LEGAL.txt	07/07/2016 05:16	Text Document	1 KB
	LICENSE.txt	07/07/2016 05:16	Text Document	15 KB
	README.txt	24/12/2016 16:13	Text Document	32 KB
	volatility_2.6_win64_standalone.exe	27/12/2016 18:02	Application	15,424 KB

עבודה עם DumpIt.exe

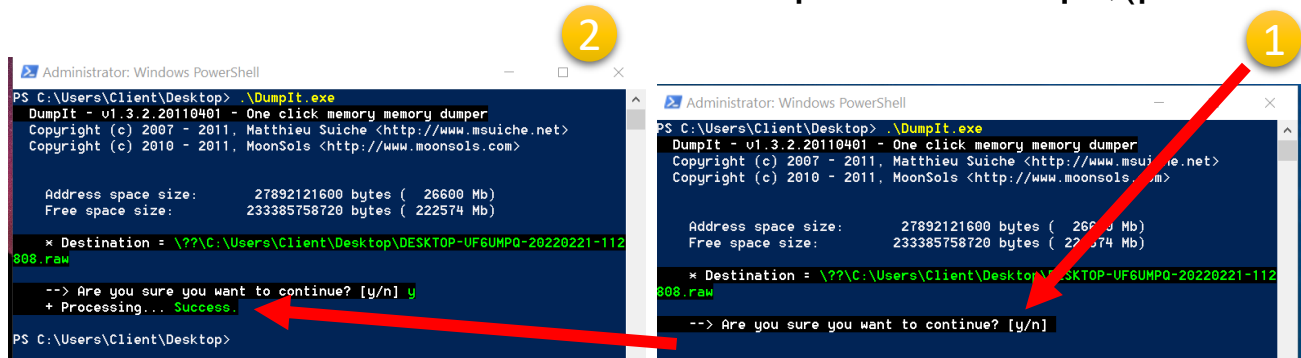
יצוא הזיכרון לקובץ חקירה - dump Image OR RAM

כאן נלמד איך מחלצים את הזיכרון במחשב שלך שניתן יהי לחקור אותו, ניתן להוריד [מכאן](#) את התוכנה dumpit.exe לחילוץ הזיכרון. עכשיו אראה לך איך לייצר קובץ dump image or ram שכזה במחשב שלך.

- אני מוריד ושם את התוכנה dumpit.exe בשולחן עבודה ופותח אותה ב חלון CMD/PowerShell



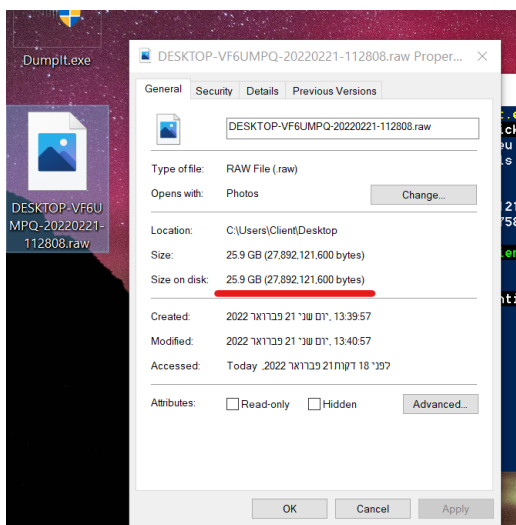
- תמונה מספר 1- לוחץ Enter, ומתקבל החלון הבא ששואל אותי האם אני מוכן להוציא את הזיכרון החוצה בנתיב הזה (בצבע ירוק), כן או לא ? ונלחץ Y + Enter



- תמונה מספר 2- אנחנו רואים שהסתיים הוצאת הזיכרון בסימון השורה : **Success.** + Processing...



וכך בשולחן עבודה נראה קובץ תמונה שהוא קובץ הזיכרון שקיבלנו, ניתן לפתוח ולראות את הגודל שלו ולשים לב שהוא מקבל משקל של גודל הזיכרון RAM של המחשב שלך אך לא בהכרח.



עבודה עם Volatility

לידע: קובץ החקירה שלי- אחרי שהפעלנו את הכלי אנחנו צריכים את הקובץ DUMP של ה RAM לחקירה שלנו ולכן אני הבאתי קובץ עם פרמטרים מעניינים לחקירה שלי ואדגים את זה, ניתן להוריד אותו מפה

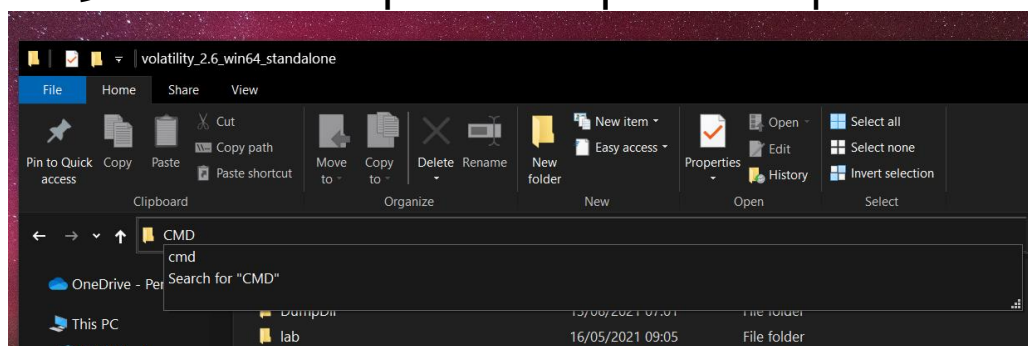
• https://drive.google.com/file/d/1LPnJ-ASqDw7m6XWvKFr_v5TGAO59pzns/view?usp=sharing

לאחר מכן לחלץ את הקובץ לתיקייה בלשולחן העבודה וניכנס לתיקייה

הפעלת הכלי-

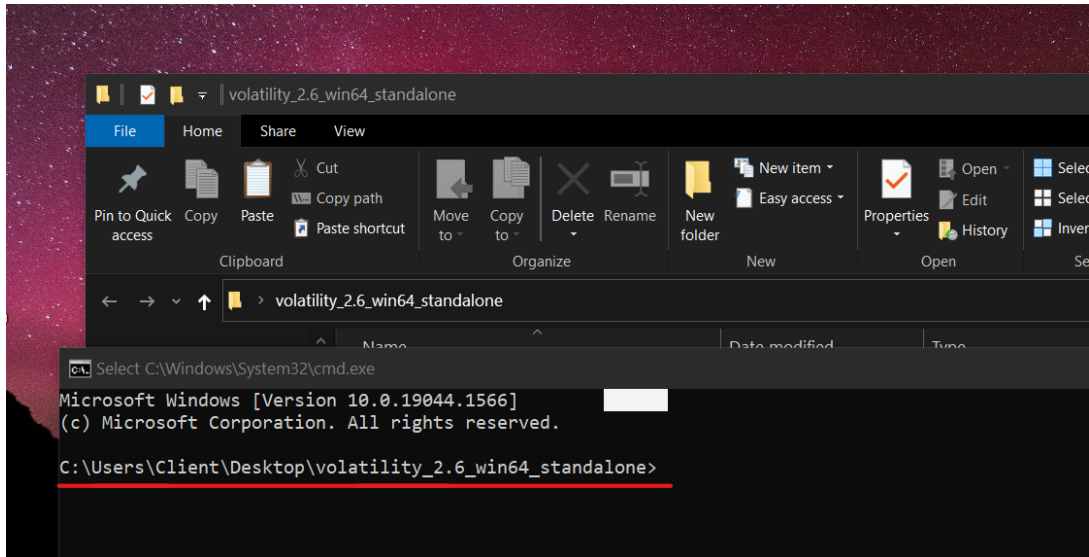
נכנסים לתיקייה וכותבים בשורת הכתובות של חלון התיקייה CMD ולאחר מכן יעלה לנו חלון 'שורת הפקודות ה cmd' בנתיב המקומי של התיקייה שלנו וכך נוכל להריץ את התוכנה ולעבוד

בה





ואז נקבל את חלון ה CMD הבא כאשר הוא מנותב ומוכן לפעולה,

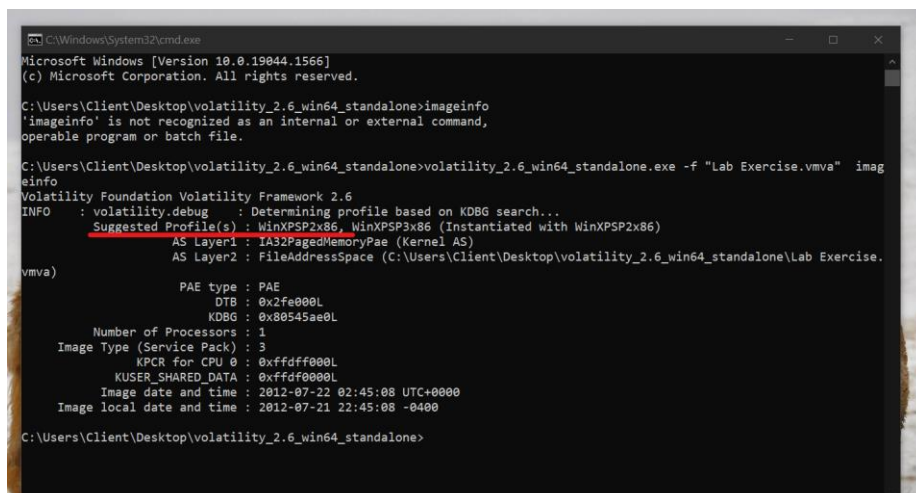


שימוש בכלי Volatility

1. טעינת קובץ-

ראשית נטען את הקובץ לחקירה ע"י הפקודה הבאה
volatility_2.6_win64_standalone.exe -f "Lab Exercise.vmva" imageinfo

- נשים לב לסוג מערכת ההפעלה הנחקרת שלנו ולעוד איבנטיים לצורך בירור מעמיק על תמונת הזיכרון,
- אני כבר לקחתי את הפרופיל המסומן באדום לחקור אותו ספציפית מתוך הזיכרון [בדור"כ תבחרו את הפרופיל הראשון זה עובד טוב יותר אך במחקר מעמיק זה מחייב לבדוק יותר]





2. מראה את התהליכים-

- אני מכניס את הפקודה הבאה שהיא מיועדת לקרוא את התהליכים שרצים בתוך תמונת הזיכרון הזה, `volatility_2.6_win64_standalone.exe -f "Lab Exercise.vmva" --profile=WinXPSP2x86 pslist`

- ידע ראשוני:** אני מתחיל לקרוא את התהליכים מתוך הפרופיל הזה ואני רואה שיש שתי שורות **PID&PPID** שהם מסמנים את התהליכים שקיימים במערכת.
- לכל תהליך במערכת יש מספר שמסמן אותו במערכת בשל ריבוי תהליכים, תהליך האב הוא תחת שורת **PID** ותהליך הבן הוא תחת **PPID** (ויכול להיות כמה וכמה תתי תהליכים)
- בבן הוא מפיק יותר תהליכים בשם האב שהאב פותח תהליכים וזה משרשר אחריו וכך ניתן לראות דוגמא בצבע ירוק בתמונה
- צריך להבין ש הכל מתחיל **בתוכנה** שרצה במחשב והיא מסומנת תחת NAME בצבע ירוק ואז נפתח מספר PID ולאחר מכן עוד תתי תהליכים ב PPID וכך ניתן לראות את התהליך מתחיל ומסתיים, זה מסומן בירוק באותו מספר שמקשר את האב לבנו

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x23c8...	System	4	0	53	240	-----	0		
0x22f1920	smss.exe	368	4	3	19	-----	0	2012-07-22 02:42:31 UTC+0000	
0x22a0598	csrss.exe	584	368	9	326	0	0	2012-07-22 02:42:32 UTC+0000	
0x2298700	winlogon.exe	608	368	23	519	0	0	2012-07-22 02:42:32 UTC+0000	
0x1e2ab28	services.exe	652	608	16	243	0	0	2012-07-22 02:42:32 UTC+0000	
0x1e2a3b8	lsass.exe	664	608	24	330	0	0	2012-07-22 02:42:32 UTC+0000	

3. מראה את התהליכים בהיררכיה-

- בפקודה הזאת ניתן לראות את התהליכים בצורה ויזואלית מסודרת יותר כמו עץ וענפים

`volatility_2.6_win64_standalone.exe -f "Lab Exercise.vmva" --profile=WinXPSP2x86 pstree`

- כאשר הנקודות בתחילת השורה מסמנות את ההקשר של תהליך האב לבנו לדוגמא כאן במסומן בירוק

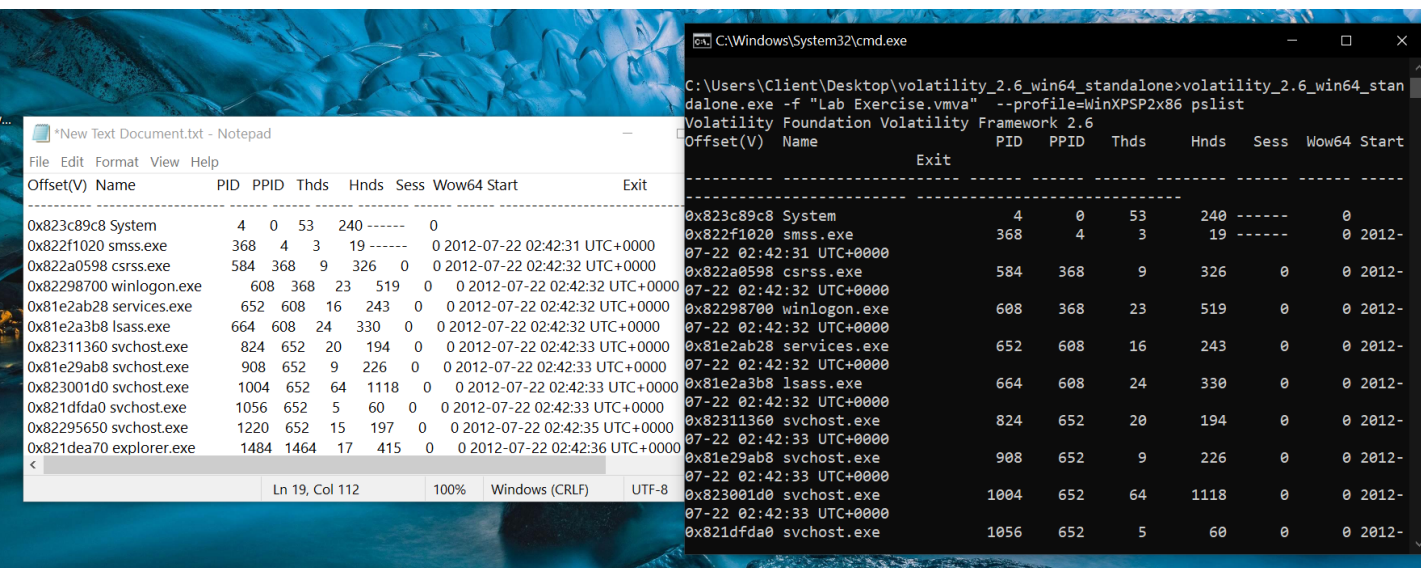
Name	Pid	Ppid	Thds	Hnds	Time
0x23c89c8: System	4	0	53	240	2012-07-22 02:42:31 UTC+0000
0x22f1920: smss.exe	368	4	3	19	2012-07-22 02:42:31 UTC+0000
0x2298700: winlogon.exe	608	368	23	519	2012-07-22 02:42:32 UTC+0000
0x1e2ab28: services.exe	652	608	16	243	2012-07-22 02:42:32 UTC+0000
0x22a0598: csrss.exe	584	368	9	326	2012-07-22 02:42:32 UTC+0000
0x1e2a3b8: lsass.exe	664	608	24	330	2012-07-22 02:42:32 UTC+0000

מכאן אנחנו נתחיל לחקור תהליכים ולמצוא תהליך זדוני שהיה קיים בתוך קובץ הזיכרון הזה!

איך נחקור?

אנחנו רואים בצורה יבשה תהליכים שרצו בזיכרון אין לנו הבנה ישירה מי הם? ולמה הם רצו?

- **התשובה היא כאן - תחילה נבין: יש תהליכים במערכת שהם תהליכים קבועים של המערכת מהיצרן! ויש שלא קבועים במערכת מתוכנות חיצוניות!**
- **אצלנו ב Windows התהליכים הקבועים האלה נבנו ע"י מהנדסי ה Windows מבית מיקרוסופט ובלעדי תהליכים אלה המערכת לא הייתה עובדת בכלל והם לא ניתנים לשינוי והם בסיס המערכת! ורק כך המערכת הזאת עולה ועובדת ולעומת זה יש תהליכים שלא רלוונטיים למערכת ההפעלה שהם חיצוניים מכל מיני יצרני תוכנות למיניהם.**
- **נתחיל לחקור ע"י שאנחנו נתחיל למפות את התהליכים בעזרת העתקת התהליכים לקובץ TXT (בעזרת מקשים אלה במקלדת תעתיק את שמות התהליכים נבחר הכל ב CTRL+A, לאחר מכן נעתיק אותם בעזרת CTRL+C ולאחר מכן נדביק בקובץ ה txt) וכך זה נראה,**



The screenshot shows a Windows desktop with a blue background. In the foreground, there is a Notepad window titled "New Text Document.txt - Notepad" and a Command Prompt window titled "C:\Windows\System32\cmd.exe".

The Notepad window displays the output of the 'pslist' command, showing a list of running processes. The output is as follows:

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x823c89c8	System	4	0	53	240	-----	0		
0x822f1020	smss.exe	368	4	3	19	-----	0	2012-07-22 02:42:31 UTC+0000	
0x822a0598	csrss.exe	584	368	9	326	0	0	2012-07-22 02:42:32 UTC+0000	
0x82298700	winlogon.exe	608	368	23	519	0	0	2012-07-22 02:42:32 UTC+0000	
0x81e2ab28	services.exe	652	608	16	243	0	0	2012-07-22 02:42:32 UTC+0000	
0x81e2a3b8	lsass.exe	664	608	24	330	0	0	2012-07-22 02:42:32 UTC+0000	
0x82311360	svchost.exe	824	652	20	194	0	0	2012-07-22 02:42:33 UTC+0000	
0x81e29ab8	svchost.exe	908	652	9	226	0	0	2012-07-22 02:42:33 UTC+0000	
0x823001d0	svchost.exe	1004	652	64	1118	0	0	2012-07-22 02:42:33 UTC+0000	
0x821dfda0	svchost.exe	1056	652	5	60	0	0	2012-07-22 02:42:35 UTC+0000	
0x82295650	svchost.exe	1220	652	15	197	0	0	2012-07-22 02:42:35 UTC+0000	
0x821dea70	explorer.exe	1484	1464	17	415	0	0	2012-07-22 02:42:36 UTC+0000	

The Command Prompt window shows the command 'volatility 2.6_win64_standalone.exe -f "Lab Exercise.vmva" --profile=WinXPSP2x86 pslist' and its output, which is a list of running processes in a similar format to the Notepad window.



- **נתחיל לחפש את התהליכים של ווינדוס** ונמפה את השאר, נחפש בגוגל את צמד המילים: Windows XP default Processes List ונמצא תוצאות שיביאו לנו את רשימת התהליכים לפי סוג המערכת שלנו,
- יש אתר מעולה בנותן תוצאות בנושא [Windows System Processes — An Overview For Blue Teams | by Nasreddine Bencherchali | Medium](#)
- נשווה את התהליכים בגוגל ונחפש את המקור של כל תהליך אם הוא רשמי ממיקרוסופט או שהוא חיצוני וע"י כך נתחיל לברר מי הם התהליכים הלא קבועים במערכת ונתחיל לחקור את הנוזקה במערכת, כך נראה השוואת תהליכים בגוגל מתהליך שהיה בזיכרון לתהליך המקורי של המערכת

The image shows a Windows XP desktop with a task manager window open, displaying a list of running processes. A green box highlights 'csrss.exe' with PID 584. A green arrow points from this box to a web browser window showing 'Default-Prozesse und andere wichtige Prozesse in Windows XP (SP2)'. The browser window lists various system processes like 'Alg.exe', 'Csrss.exe', and 'Ctfmon.exe' with their respective contexts and functions.

- **שימו לב לדבר מעניין**, מצאתי שהתהליך הזה reader_sl.exe הוא לא מוכר כתהליך מקורי בווינדוס,
- זה תהליך שהגיע מבחוץ דרך הדפדפן ושמותי לב לזה בגלל תהליך האב explorer.exe 1484 שהוא reader_sl.exe 1484 שכרגע אינו ידוע לנו,

The image shows a Notepad window titled '*blacklist.txt - Notepad'. It contains a table of processes with their PIDs and PPIDs highlighted in orange.

	PID	PPID	
0x821dea70:explorer.exe	1484	1464	17 415 2012-07-22 02:42:36 UTC+0000
0x81e7bda0:reader_sl.exe	1640	1484	5 39 2012-07-22 02:42:36 UTC+0000

- **אבל התוכנה** שיוצרת כאן את התקשורת היא הבן reader_sl.exe ולא הדפדפן היות ודפדפן לא יוצר תקשורת סתם כך לבחוך. זה תוכנה שמחייבת אותו כאן לייצר תקשורת ל בחוץ ואם כך זה מתהפך לנו בהבנה שמי שכאן הוא האב זה reader_sl.exe והבן הוא explorer.exe ולכן נפנה לחקור את תקשורת המחשב להבין מי זה התהליך הזה אולי הוא זדוני!

לחקור את התקשורת של המחשב עם עולם החיצון.

- הפקודה הזאת מאפשרת לצפות בתקשורת רשת שהתקיימו בתחנה

`volatility_2.6_win64_standalone.exe -f "Lab Exercise.vmva" --profile=WinXPSP2x86 connscan`

- לאחר שעשינו בדיקה וראינו תקשורת בין התחנה לאינטרנט אנחנו מבינים שיש כאן תקשורת לא תקינה של קובץ שמפעיל דפדפן לתקשר לבחוץ וכך נחקרו לעומק את החשדות האלה בעזרת חקירת הכתובות,

- לאחר שהבנו שהכתובת המקומית של המחשב היא

172.16.112.128 יוצרת תקשורת עם כתובת מרוחקת

41.168.5.140 בפורט **8080**, זה לא יכול לקרות סתם כך

היות ודפדפן לא יוצר תקשורת סתם כך ל בחוץ ותקשורת

צריכה להיעשות בידי אדם וכאן זה תוכנה שמחייבת אותו

לייצר תקשורת ל בחוץ ואם כן אני מבין ש **explorer.exe** הוא

הבן והוא מופעל ע"י תהליך האב **reader_sl.exe** וזה

מתחיל להחשיד שיש כאן תוכנה שמפעילה תקשורת כלפי

חוץ וזה מאפיין תוכנה זדונית

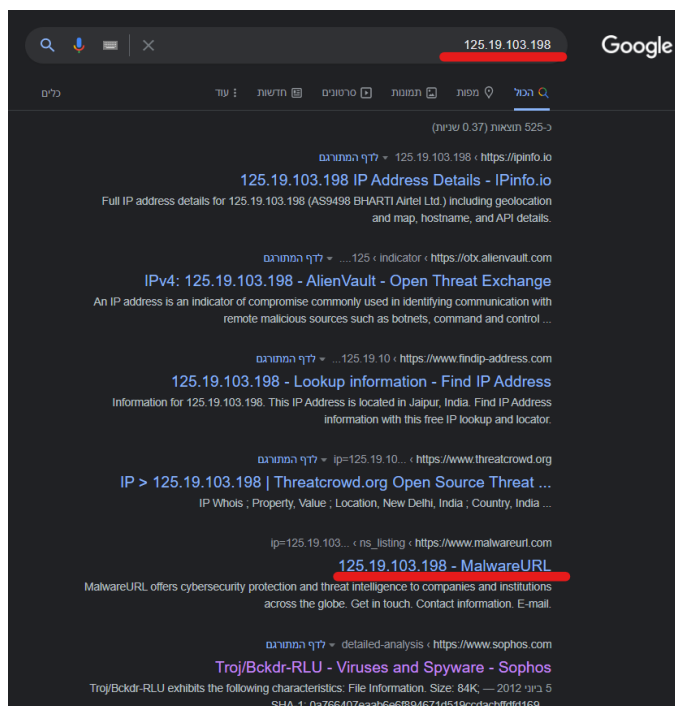
כתובת
מקומית

כתובת
מרוחקת

```
C:\Users\Client\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f "Lab Exercise.vmva" --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P) Local Address Remote Address Pid
-----
0x02087620 172.16.112.128:1038 41.168.5.140:8080 1484
0x023a8008 172.16.112.128:1037 125.19.103.198:8080 1484
C:\Users\Client\Desktop\volatility_2.6_win64_standalone>
```

- לכן נפנה לחפש בגוגל את הכתובות האלה ונראה אילו דוחות ותוצאות נכתבו על כתובות אלה,

- נשים לב להתייחסות כללית: בתוצאות של גוגל לכתובות אלה באדום וזה מראה לנו שיש דוחות שלמים ומאמרים שנכתבו ומעידים על סוס טרויאני שמסתתר בתקשורת של הקובץ הזדוני במערכת אל התקשורת הסופית בכתובת הזאת והמשנה שלה,



- נשים לב להתייחסות ישירה לנוזקה שלנו: באתר virus total אנחנו רואים תוצאה שמשימה לנו את החקירה בהבנה שהחשד הראשוני שהיה לי שהתהליך reader_sl.exe בזיכרון הוא מתנהג בצורה מחשידה וכופה על הדפדפן להוציא תקשורת ל בחוץ התברר כנכון וקיבלנו מידע ודו"ח מדויק מ virus total על הכתובת והקובץ שהינו סוס טרויאני וניתן לראות את זה בחקירה פיזית בהמשך...

41.168.5.140				5			
41.168.5.140 (41.168.0.0/15)				5 security vendors flagged this IP address as malicious			
AS 36937 (Neotel)				ZA			
Community Score				DETECTION			
Avira	Malware	CRDF	Malicious	DrWeb	Malicious	Fortinet	Malware
Webroot	Malicious	Abusix	Clean	Acronis	Clean	ADMINUSLabs	Clean



כיוון נוסף לחקירה פיזית בזיכרון

- זה האפשרות לחלץ את התהליך החשוד ולבדוק אותו פיזית באתר Virus total ולשם כך נייצא את התהליך הזדוני שמצאנו,

איך לייצא תהליך ?

- כך נייצא תהליך ספציפי- (חובה לחלץ תהליך אב! ולא תתי תהליכים).
- לצורך חילוץ נפתח תיקייה ונקרא לה בשם מסוים וכך ננתב את חילוץ התהליך לתיקייה כמו אצלי;

```

C:\Users\Client\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f "Lab Exercise.vmva" --pr
ofile=WinXPSP2x86 procdump -D dumpdir -p
  
```

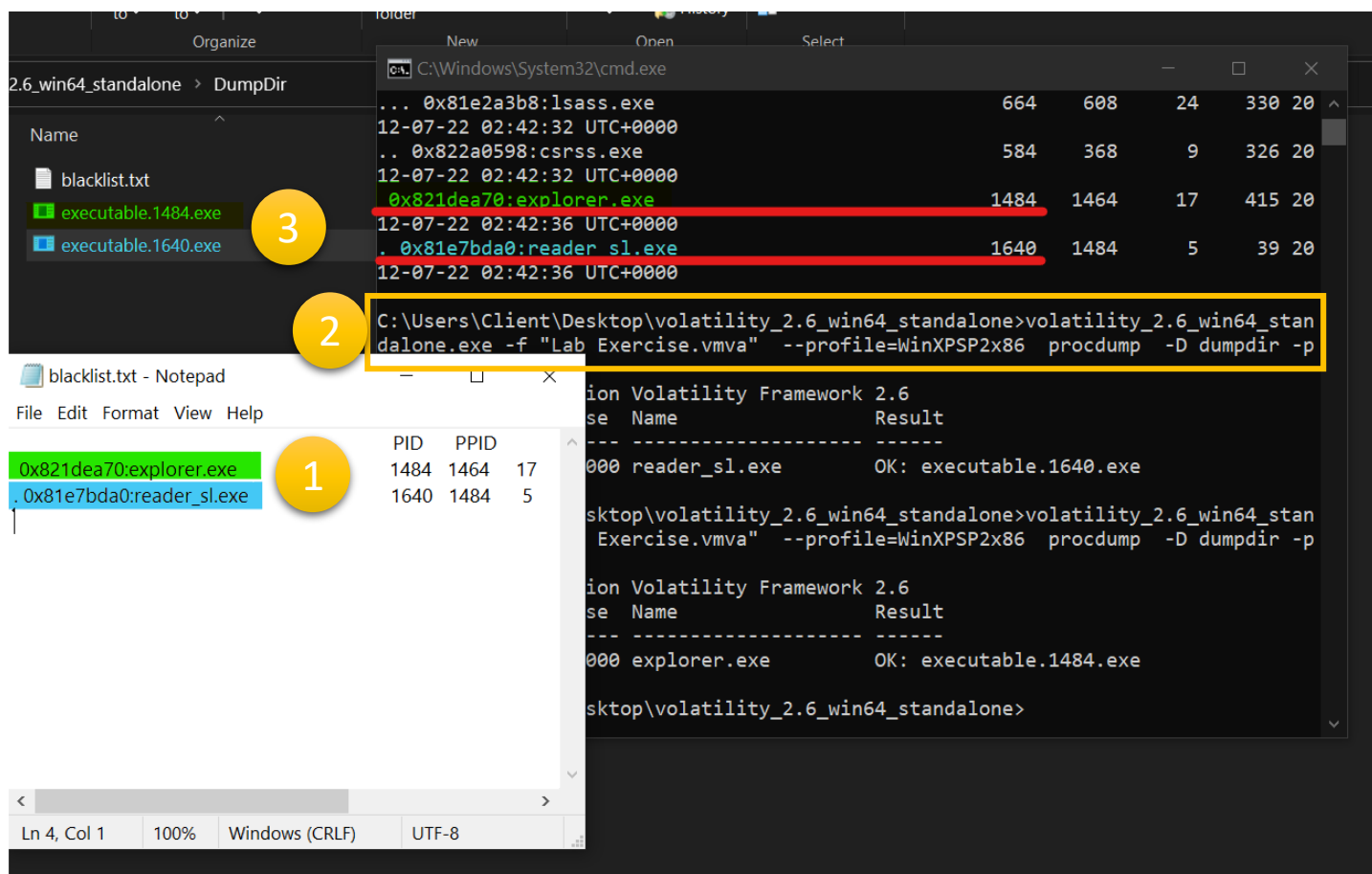
- בפקודה הזאת אנחנו נחלץ תהליך ספציפי ונחקור אותו, **volatility_2.6_win64_standalone.exe -f "Lab Exercise.vmva" --profile=WinXPSP2x86 procdump -D dumpdir -p** (בתוספת מספר תהליך האב)
- ניתן לראות את החילוץ של הקובץ ע"י הפקודה, ולראות את הקובץ שחולץ בתיקייה.

```

C:\Users\Client\Desktop\volatility_2.6_win64_standalone> volatility_2.6_win64_standalone.exe -f "Lab Exercise.vmva" --pr
ofile=WinXPSP2x86 procdump -D dumpdir -p 368
  
```

ייצוא התהליך הזדוני שלנו

1. לאחר הפילטור של תהליכים ששייכים ל Windows שעשיתי לעיל ניתן לראות את התהליכים הלא מוכרים ב TXT ,
2. ניתן לראות שאני מחלץ את התהליכים הנ"ל ע"י הפקודה לחילוץ תהליכים,
3. וניתן לראות את התהליכים שחולצו בתיקייה במספר ה PID שלהם



The screenshot shows the Volatility framework output and a Notepad window. The output displays a list of processes with their PIDs and PPIDs. The Notepad window shows the results of the dumpdir command, listing the processes and their corresponding executable files.

Volatility Framework Output:

Process Name	PID	PPID
0x81e2a3b8:lsass.exe	664	608
12-07-22 02:42:32 UTC+0000		
.. 0x822a0598:csrss.exe	584	368
12-07-22 02:42:32 UTC+0000		
0x821dea70:explorer.exe	1484	1464
12-07-22 02:42:36 UTC+0000		
.. 0x81e7bda0:reader_sl.exe	1640	1484
12-07-22 02:42:36 UTC+0000		

Notepad Output (blacklist.txt):

```

PID      PPID
-----
0x821dea70:explorer.exe 1484 1464 17
0x81e7bda0:reader_sl.exe 1640 1484 5
  
```

Volatility Framework Command and Output:

```

C:\Users\Client\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f "Lab Exercise.vmva" --profile=WinXPSP2x86 procdump -D dumpdir -p

Volatility Framework 2.6
Process Name      Result
-----
000 reader_sl.exe OK: executable.1640.exe

C:\Users\Client\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f "Lab Exercise.vmva" --profile=WinXPSP2x86 procdump -D dumpdir -p

Volatility Framework 2.6
Process Name      Result
-----
000 explorer.exe  OK: executable.1484.exe

C:\Users\Client\Desktop\volatility_2.6_win64_standalone>
  
```

- לאחר מכן אני מעלה את הקבצים האלה לאתר Virus total ורואה את התוצאה
- ניתן לראות שהחשד בחקירה שלנו נכונה היות והקובץ עצמו הועלה ידנית ונבדק בשירות של virus total ושם אנחנו רואים דוחות שלמים באתר על המחקר שעשיתי כאן אתכם.
- תוצאה 1 של: PID 1640 reader_sl.exe כפי שמוצג לנו מ [virus total](#)
- תוצאה 2 של: PID 1484 explorer.exe כפי שמוצג לנו מ [virus total](#)

5b136147911b041f0126ce82dfd24c4e2c79553b65d3240ecea2dcab4452dcb5

1

31 / 68

31 security vendors and no sandboxes flagged this file as malicious

5b136147911b041f0126ce82dfd24c4e2c79553b65d3240ecea2dcab4452dcb5

AcroSpeed.Launch.exe

28.50 KB

2022-02-03 06:45:22 UTC

21 days ago

EXE

Community Score

direct-cpu-clock-access

idle

peexe

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Trojan.GenericKD.41512677	Alibaba	① Trojan.Win32/Multiop.788dce0e	
ALYac	① Trojan.GenericKD.41512677	Arcabit	① Trojan.Generic.D2796EE5	
BitDefender	① Trojan.GenericKD.41512677	Comodo	① Malware@#b21hr9e1xviv	
Cybereason	① Malicious.3f5a91	Cylance	① Unsafe	
Emsisoft	① Trojan.GenericKD.41512677 (B)	eScan	① Trojan.GenericKD.41512677	
Fortinet	① PossibleThreat	GData	① Trojan.GenericKD.41512677	
Ikarus	① Trojan.Win32.Patched	K7AntiVirus	① Riskware (0040eff71)	
K7GW	① Riskware (0040eff71)	Kingsoft	① Win32.Troj.Generic_a.a.(kcloud)	
Lionic	① Trojan.Win32.Generic.41c	MAX	① Malware (ai Score=99)	

48db195007e5ae9fc1246506564af154927e9f3fbfca0b4054552804027abbf2

2

18 / 68

18 security vendors and no sandboxes flagged this file as malicious

48db195007e5ae9fc1246506564af154927e9f3fbfca0b4054552804027abbf2

executable.1484.exe

1009.50 KB

2021-12-26 05:20:06 UTC

2 months ago

EXE

Community Score

idle

peexe

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Alibaba	① RiskWare:Win32/Multiop.1bca5b26	Antiy-AVL	① Trojan/Generic.ASMalwS.494CA6	
Cybereason	① Malicious.838345	Cylance	① Unsafe	
Ikarus	① Trojan-Dropper.Agent	K7AntiVirus	① Riskware (00584baa1)	
K7GW	① Riskware (00584baa1)	Kaspersky	① Not-a-virus:RiskTool.Win32.Agent.amvb	
Lionic	① Riskware.Win32.Agent.11c	McAfee	① Artemis!F5D61A0CCF96	
McAfee-GW-Edition	① BehavesLike.Win32.Dropper.fz	Microsoft	① Trojan.Win32/Multiop	
Palo Alto Networks	① Generic.ml	Rising	① Trojan.Generic@ML.88 (RDML:PFex5ibh2...	
Trellix (FireEye)	① Generic.mg.f5d61a0ccf96e072	VIPRE	① Trojan.Win32.Generic!BT	
Webroot	① W32.Trojan.Multiop	Zillya	① Tool.Agent.Win32.31388	

Memory Forensics - Volatility



כל הזכויות שמורות ליוצר [LinkedIn](#)

רישיון (CC BY-NC-SA) ייחוס, ללא שימושים מסחריים ושיתוף ברישיון זהה) - מאפשר לכם להשתמש ולשתף את התוכן, כל עוד אתם נותנים קרדיט ליוצר המקורי, תוך התחייבות שלא תשתמשו בתוכן למטרות מסחריות. כמו כן אתם בתורכם תשתפו את התוכן תחת אותו רישיון.

