Digital forensics drill down - Lone Wolf

תקציר
טרור זאב בודד נחשב לאיום חמור על ביטחון הציבור בשנים האחרונות ונראה שהתופעה גוברת בקצב מדאיג. נקודת מבט אחת המודגשת בחקירה היא השימוש ברשת האינטרנט על מנת לתכנן פיגועים. הם מקושרים, מרושתים, מחוברים, מתקשרים ומשתפים ידע והדרכה באמצעות האינטרנט. ניתוח של כל המקרים האחרונים, הדוחות והמחקרים של אנשים אלה חושפים את הסיכון בזאבים בודדים ברשת האינטרנט, כולל מדיות חברתיות (פייסבוק, אינסטגרם, יוטיוב ועוד).

מבוא
האיום הרציני מגיע מהזאב הבודד, הוא קיצוני באינטרנט, ומתכנן לפגוע בכל מי שחושב אחרת. הוא משתמש בטקטיקות טרור לכל דבר על מנת להשיג מטרות אידיאולוגיות ו\או פוליטיות (בין אם בשיתוף פעולה עם ארגון טרור רשמי או לא רשמי, תא או קבוצה).
המטרה בחקירה הזאת, היא היכולת לחשוף את הזאבים הבודדים בתקשורת ובפלטפורמות הדיגיטליות השונות. הניתוח מבוסס על בסיס דיסק וזיכרון ממחשב נייד שנאספו מהחשוד בצו בית משפט.
רשתות חברתיות הפכו למנגנון טרור רב עוצמה. קהילות וירטואליות גדלות והופכות לפופולריות בעולם ובמיוחד בקרב צעירים. קבוצות טרור ג'יהאדיסטיות פונות בעיקר לבני נוער למטרות תעמולה, הסתה וגיוס ובהתאם לכך, ארגוני טרור ואוהדיהם מנצלים יותר ויותר את הרשת בעיקר בקהילות כמו פייסבוק, Myspace. "הפורום על תפקיד האינטרנט במאבק בטרור והקצנה" שנערך בערב הסעודית בינואר 2011 התמקד באופן שבו המדיה החברתית המקוונת תרמה לעלייה ב"זאבים בודדים". הסיבה לכך היא שיחידים המדברים על דעותיהם הקיצוניות באופן אישי יכולים למצוא בקלות אנשים דומים דרך צ'אטים ופורומים, ובאמצעות קשרים וירטואליים, הם מקבלים מספיק ביטחון לבצע פעולות טרור.

אתרי מדיה חברתית (בעיקר) פונות לקהל הרחב, כולל אנשים שאין להם חיבור לארגוני טרור. לכן, מרבית הפורומים מגבילים את הגישה (לחלוטין או חלקית) ומאפשרים כניסה רק לאנשים שצריכים להוכיח את נאמנותם, או דרך המלצה אישית של חברים. בנוסף, המנחים ממליצים בחום להשתמש בהצפנת תוכנה עבור תקשורת ישירה.

תפקיד האינטרנט לזאב הבודד
האינטרנט הוא כלי יעיל מאוד לזאב הבודד: מספק גישה ישירה לאנשים בעלי דעות דומות בכל רחבי העולם איתם הם יכולים להתחבר ובמקרים מסוימים יכול לספק להם הנחיה לפעילויות. הקהילה יכולה לשמש כסביבה חברתית חלופית שהם אינם מסוגלים לה בעולם האמיתי. שירות המודיעין והביטחון של הולנד (AIVD) הגיע למסקנה דומה: רדיקליזציה היא תופעה חברתית - זאבים בודדים לעתים קרובות מתכננים ומבצעים פעולה אלימה יחד. לעתים קרובות רואים שזאבים בודדים כמעט ולא היו עם דעות דומות בחיים האמיתיים, אך כן שמרו על קשר פעיל באינטרנט. היום מבינים שמגעים אלה (בנוסף לצריכת תעמולה ג'יהאדיסטית) תרמו להקצנתם והעניקו להם השראה לבצע פעולת טרור.

דו"ח מודיעיני של מרכז הערכת האיומים המשולב של ממשלת קנדה הביע דאגה מהאיום המתגבש שמעלים זאבים בודדים אסלאמיסטיים. הדו"ח הדגיש את חשיבות האינטרנט: האינטרנט מועיל לאדם שעשוי לבצע התקפת זאב בודד, במתן מוטיבציה אידיאולוגית, הצדקה לפעולה וכל זאת באנונימיות מוחלטת. אתרי אינטרנט קיצוניים אסלאמיסטיים מציעים לא רק הדרכה תיאורטית ודתית, אלא גם קורסים מעשיים. לדוגמה: האנציקלופדיה המקיפה להכנה לג'יהאד זמינה ברשת, יש שם חומרי הדרכה מקצועיים בווידיאו שמראים חומרי נפץ שונים וגם מתכונים לייצור (יחד עם עשרות מדריכי טרור אחרים). דוח הטרור שפורסם באפריל 2012, הדגיש את חשיבות האינטרנט. הדו"ח קובע כי האינטרנט הפך לאמצעי תקשורת עיקרי ושלאינטרנט יש פוטנציאל להתקפות סייבר על תשתיות ברחבי העולם. כמעט כל המקרים של זאב בודד בשנים האחרונות היו כרוכים בשימוש במדיה חברתית. עבור זאבים בודדים, תקשורת ברשת מספקת קשר חברתי, קהילה, מקור הדרכה, תמיכה וגיבוי מוסרי.

דוגמה להמחשה: בשנת 2011 נעצר בחור בשם חוזה פימנטל על תכנון פיגועים נגד ניידות משטרה ומתקני דואר בניו יורק ובניו ג'רזי בעזרת מטעני צינור תוצרת בית. פימנטל, יליד הרפובליקה הדומיניקנית הגיע לארה"ב בגיל 8 והיה מוסלמי מובטל, בן 27 שחי במנהטן ואוהד של אל-קאעידה. הוא הואשם בחמישה סעיפים של בניית מטעני צינור המיועדות לחיילים שחזרו מעיראק ואפגניסטן. פימנטל לא היה חלק מאף ארגון ידוע של אל-קאעידה. למרות זאת, ההשראה להתקפות ההפצצה המתוכננות שלו נבעה מהוראות קריאה במגזין בשם Inspire שהופק על ידי אל-קאעידה. החוקרים גילו שפימנטל מצא במגזין את ההוראות לבניית המטענים. ההוראות היו במאמר "איך להכין פצצה במטבח של אמא". הקריאה במגזין לא הייתה הפעילות הרשתית העיקרית שלו - הוא צפה וכתב באתר Blogger שמציג מאות מאמרים רדיקלים. בחקירה פורנזית של פימנטל התגלה כי הוא התחבר לרשת קיצונים ידועים המכילה כמה מאות אנשים דומים בדעות. באתר TrueIslam1.com, פימנטל אירח ארכיון מרשים של מאמרים וסרטונים ג'יהאדיסטיים, שהועלו באתר Blogger. האתר התחבר לערוץ היוטיוב של פימנטל (שהיו יותר מ -1,500 מנויים), ששם מצאו יותר מ- 600 סרטונים המתייחסים לרדיקלים אלימים ופרשנויות לאסלאם, כש-60 מהם העלה בעצמו.

טרוריסטים רותמים את היכולות האינטראקטיביות של חדרי צ'אט, מסנג'ר, בלוגים, אתרי שיתוף וידאו, קבוצות מקוונות ורשתות חברתיות. כיום, 90% מפעילות הטרור באינטרנט מתרחש באמצעות רשת חברתית, פורומים משמשים כ-FW וירטואלי שמסייע לשמירה על זהות המשתתפים והם גם מציעים למנויים אפשרות ליצור קשר ישיר עם טרוריסט, נציגים, לשאול שאלות ואפילו לתרום ולעזור לג'יהאד הסייבר. גם דובר החמאס ציין בהודעה רשמית בטוויטר את כוחן של הרשתות החברתיות: "אנו קוראים לאמץ אסטרטגיה על בסיס התנגדות ושמירה על זכויותינו וקביעותינו". אמנם הצהרות תמיכה ב"התנגדות" עשויות להיות מיושנות, אך הנהגת החמאס מנצלת את המדיה החברתית בכדי להגיע לקהל חדש וכוללת חשבונות ב- YouTube, Flickr, Twitter ו- Facebook, כמו גם אתר 'www.hamasinfo.net ופורומים שונים. בדומה לחמאס, גם החיזבאללה הקים רשת עצומה של פעילים ברחבי אמריקה הלטינית וצפון אמריקה. הרשת יכולה לשמש למתן הוראה לביצוע פיגועים אם רק ירצו. פרסומים בפורומים כאלה קוראים להתקפות של זאבים בודדים ובנוסף תוארו פיגועי ירי כנקמתו של אללה בצרפת על מדיניות החוץ ויחסה למוסלמים.

מסקנות

הגידול המשמעותי בטרור של זאב בודד מוסבר על ידי שימוש בפלטפורמות רשתיות שונות ומגוונות להפצת טקטיקות של זאב בודד. קבוצות טרור למדו כיצד לפנות לזאבים בודדים פוטנציאליים ולפתות אותם, לאמן וללמד אותם ולבסוף לשלוח אותם להתקפות והכל באמצעות פורומים, צ'אטים, פייסבוק, יוטיוב, טוויטר ועוד. טרור של זאבים בודדים מספק את הטרור המאתגר ביותר. הם סיוט עבור ארגוני ה-CT (Counter Terror) כגון המשטרה וקהילות המודיעין מאחר שקשה מאוד למצוא, לזהות ולעצור אותם. עם זאת, העובדה שזאבים בודדים אינם לגמרי לבד עשויה להוביל לצעדים מניעתיים. הגורם המרכזי באיתור טרור זאבים בודדים היא ללמוד ולדעת את תהליכי ההקצנה של זאבים בודדים. ההבנה לתהליכים האלה פותחת דרכים אפשריות לצעדים יעילים למניעת טרור זאב בודד. אם תהליך הגיוס, התמיכה וההכשרה בזאבים בודדים מסתמך על הרשת, אפשר ללמוד ולפקח על אתרים חשודים. ההסברה של קהילות טרור רדיקליות, קיצוניות, ג'יהאדיסטיות ואחרות היא המפתח לסימנים מקדימים לרשויות החוק. סימנים כאלה כוללים קשרים שאנשים יצרו עם רדיקלים ידועים או אינטראקציה כלשהי באתרים רדיקליים. משטרת ניו יורק פיתחה יחידת מודיעין סייבר, "סוכני סייבר" סמויים עוקבים אחר הפעילות המקוונת של חשודים קיצוניים ומתקשרים איתם ברשת כדי לאמוד את המסוכנות הפוטנציאלית שלהם. היחידה מילאה תפקיד מפתח בכמה חקירות טרור, כמו של עבד אל חמד שחאדה, שניסה להגיע לסומליה כדי להילחם למען קבוצת אל-קאעידה המקומית. יחידת מודיעין הסייבר גילתה שהוא מחזיק בחומר טרור שרכש על ידי גישה למקורות ברשת. מקרים אלה מדגימים לא רק את האיום ההולך וגובר מצד אנשים בעלי רדיקליזציה עצמית ללא כל אינטראקציה פיזית עם קבוצות טרור, אלא גם על תלותן של קבוצות אלו ברשת, מה שעשוי לשמש כנגדם לטובת רשויות החוק.

תרחיש זאב בודד

התרחיש מבוסס על אדם שתכנן פיגוע ירי המוני. תכנון הפיגוע מפסיק כשהאח של החשוד מתקשר למשטרה ומתריע על פיגוע ירי שעומד להתרחש.

המטרה היא לקבוע האם החשוד אכן תכנן לבצע פיגוע ירי והאם פעל לבד כ"זאב בודד".

נתונים פליליים של החקירה

החקירה מורכבת **מדיסק וזיכרון ממחשב נייד** שנלקחו בצו בית משפט מהחשוד.

- FTK Imager Log.txt
- LoneWolf.E01
- LoneWolf.E02
- LoneWolf.E03
- LoneWolf.E04
- LoneWolf.E05
- LoneWolf.E06
- LoneWolf.E07
- LoneWolf.E08
- LoneWolf.E09
- memdump.mem
- pagefile.sys

או

- קובץ ZIP 32GB יחיד המכיל את הדיסק ותמונות הזיכרון.

זיהוי פלילי דיגיטלי ותגובה לאירועים הם תחומים מיוחדים באבטחת הסייבר אשר נמצאים בידי צוותי תגובת חירום, או בצוותי תגובה לאירועי אבטחת מחשבים.

DFIR - Digital Forensics and Incident Response

CERT - Computer Emergency Response Teams

CSIRT - Computer Security Incident Response Teams

דוחות פליליים:

התרחיש נחקר בעזרת כמה כלים:

Lone Wolf Scenario Guide.
Evidence Validation Report.
Autopsy Example Report Directory

- Autopsy Report.html
- content

Axiom Example Reports Directory

- .txt files
- Example Axiom HTML Report Directory
- Report.html
- Attachments
- Resources
- Example Axiom Pictures Report Directory
- Pictures Report.html
- Attachments
- Resources

Axiom Tagged Files Listing Directory

- .csv files

Exported Evidence Files Directory

- .ldb file
- .bin files
- .docx files
- SQLite DB file
- .pptx file
- .csv file

Forensic Image Files Directory

- LoneWolf.E01 – LoneWolf E09
- memdump.mem
- pagefile.sys
- FTK Imager Log.txt

Keylogger Report Directory

- .html files
- .jpg files

Potentially Recoverable Directory

- .txt file
- .png file
- .onepkg file
- .pdf file
- .zip file (Google Takeout Archive)

כלים ששימשו לחקירה:

חומרה, מערכות הפעלה (רצוי להשתמש במערכת הפעלה זהה לזו המשמשת את החשודים כדי שניתן יהיה ליצור את אותם התנאים), תוכנות וקבצים:

- Windows 98
- Windows ME
- Windows Home and Media
- Windows XP Pro
- Windows 2000 Professional
- Windows 2003 Server
- Linux.
- דיסק - Drive Model: Samsung SSD 850 PRO 512GB Serial Number: S250NSAG505708H
- קובץ זיכרון
- Autopsy - מאחר והוא gui (graphical user interface), אפשר לייצר קובץ מדיסק ולטעון אותו בתוכנה להקלת תהליך החקירה.
- Axiom - פלטפורמת חקירה עם יכולת לשחזור, ניתוח ודיווח נתונים (כמו תכונות ציר הזמן) ממקורות נייחים, ניידים ומעננים.
- Google Chrome
- Microsoft Edge

חומרה

- Forensic Hard Drive Duplicator - Multiple HDD Cloner & SSD Copier
שכפול משפטי מתייחס לקובץ המכיל כל פיסת מידע מהמקור בפורמט זרם סיביות גולמי (מה שאומר שגם מחיצות נסתרות יכולות להימצא על ידי המשכפל).

- השכפול נועד להעתיק את הכונן הקשיח המקורי. כל מה שצריך לעשות זה לחבר את כונן המקור ואת כונן היעד לחריץ שלהם ובלחיצת כפתור הכונן הקשיח ישוכפל. ה- Forensic Duplicator משמש גם לחסימת כל שינוי בכונן המקורי כאשר הוא מחובר למחשב דרך יציאת USB. בנוסף, הוא יכול ליירט ולחסום כל פעולת פיקוד שתגיע לכונן הקשיח על מנת למנוע שינוי נתונים כשקוראים את הכונן הקשיח מהמחשב.

ארכיטקטורת זיכרון

שיטות המשמשות לאחסון ולאחזור מידע בהתאם ליישום ספציפי על ידי שילוב בין הדרך המהירה, האמינה והעמידה לבין הדרך הזולה.

- **זיכרון מטמון** - משמש את יחידת העיבוד המרכזית (CPU) של המחשב כדי להקטין את הזמן לגישה לנתונים מן הזיכרון הראשי.
- **זיכרון ראשי** - (RAM) שניתן לגשת אליו באמצעות זיכרון המטמון או ישירות באמצעות המעבד.
- **זיכרון עזר** - אחסון משני/חיצוני. זיכרון שלא מאבד נתונים כשהמכשיר מופעל ובנוסף לא נגיש ישירות על ידי המעבד.

מפתח רישום

הרישום בזיכרון מכיל כמה מפתחות:

- **ROOT CLASSES:** מכיל מידע על סוגי קבצים, כולל אילו תוכניות משמשות לפתיחת סוג קובץ מסוים.
- **USER CURRENT:** מכיל הגדרות ספציפיות הבנויות ממידע במפתח HKEY_USERS.
- **MACHINE LOCAL**: מכיל מידע ספציפי למחשב כולל חומרה ותוכנה מותקנים.
- **USERS:** מכיל מידע על כל המשתמשים שנכנסים למחשב. מכיל מפתח אחד לכל משתמש.
- **CONFIG CURRENT:** מכיל מידע על תצורת החומרה של המחשב.

ניתן לסרוק את המפתחות באופן אוטומטי:

- פתיחת Run באמצעות win + r.
- הקלדת הפקודה "regedit".
- בחינת תוכן התיקיה.

- **קבצים פתוחים:** פותחים את כל הקבצים שיכולים לחשוף מידע המשמש לתהליך זדוני (גם אם הדיסק מוצפן ניתן יהיה למצוא את הקובץ בזיכרון לא מוצפן).
- **גרסאות לא מפוענחות:** אם קיים בכונן קובץ זדוני מוצפן, אפשר לנסות לפענח את הקובץ באמצעות ניתוח סטטי או על ידי כלי אנטי וירוס (הצעד החשוב ביותר לביצוע בפורנזיקה).
- **תוכנה זדונית:** תוכנות זדוניות מסוימות יישארו רק בזיכרון המערכת ולא ישאירו עקבות בכונן ולכן לפעמים קשה לזהות אותן.

כלי חקירה נוספים ל-Autopsy (לא נעזרתי בהם לחקירה , אך רצוי לדעת שיש עוד כלים דומים):

- IBM Security QRadar
- Forensic Toolkit
- EnCase Forensic
- X-Ways Forensics
- FireEye Network Security and Forensics
- Magnet Forensics
- Parrot Security OS
- Cyber Triage

<u>ישנן מספר דרכים לבצע חקירה פורנזית - תלוי בעיקר במידת העומק שרוצים ובכמות המידע שיש.</u>

ביצוע חקירה פורנזית מקיפה מצריכה כמה שלבים:

- שכפול כל שרת ו\או כוננים ו\או מחשבים הקשורים לאירוע. חשוב לשכפל גם את זיכרון ה-RAM וגם את הכוננים הקשיחים.
- בדיקה שכל המכשירים מכוונים על אותו הזמן בדיוק (יום, שעה ודקה).
- שמירת יומני בקרה ומעקב של תוכנות כמו Active Directory, Office, outlook/gmail (IMAP/POP3), Firewall ועוד.
- תרשים של כל נקודות היציאה והכניסה לרשת הארגונית (ראוטרים, שרתים, Firewall).
- תרשים תהליכי זרימה של המערכות שהותקפו ו\או נפגעו.
- הפרדת המערכות שנפגעו ואחסון ברשת נפרדת, שאינה מחוברת פיזית, או וירטואלית לרשת הארגונית.

טכניקות חיפוש ראיות:

- רישום קבצים: ניתוח קבצים וספריות, כולל שמות קבצים שנמחקו וקבצים עם Unicode.
- תוכן הקובץ: ניתן להציג את תוכן הקבצים ב-hex או לחלץ את המידע ב-ASCII.
- זדוני או לא: חיפוש קבצים לא ידועים ב-hash כדי לזהות אותם כזדוניים או לא.
- סוג הקובץ: מיון הקבצים לפי החתימות שלהם כדי לזהות קבצים. כולל קבצים מוסתרים.
- ציר זמן: מסייע בזיהוי קבצים שעשויים להכיל עדויות. ערכים לזמנים שהשתנו, גישה ושינוי (MAC) של קבצים.
- מילות מפתח: ניתן לבצע חיפושי מילות מפתח במערכת הקבצים באמצעות ASCII וביטויים קבועים של grep. ניתן גם ליצור קובץ אינדקס לחיפושים מהירים יותר ע"י הגדרת strings שמחפשים לעתים קרובות בחקירה ו\או חיפוש אוטומטי שיעזור למצוא מידע.
- Metadata: שימושי מאוד לשחזור תוכן שנמחק ע"י חיפוש בקבצים וספריות כדי לזהות את הנתיב המלא של הקובץ.
- יחידות נתונים: המקום בו נמצא תוכן הקובץ. ניתן להציג את התוכן בכמה פקודות אפשרויות דרך **Sleuth Kit**: Hexdump, strings, file, img_stat, fsstat, fls, istat, icat, ils, sorter, mmls, scalpel, dd
- תמונה: ניתן להציג נתונים כמו סוג, תאריך ושעת הצילום ולפעמים גם היכן צולמה התמונה (מיקום GPS).

ניהול תיקים:

- רצף אירועים: ניתן להוסיף אירועים מבוססי זמן מפעילות קבצים או מיומני IDS וה-FW. ניתן למיין את האירועים כך שניתן לקבוע בקלות את רצף האירועים הקשורים לחקירה .
- דוחות: ניתן להפיק דוח ASCII על מנת לנהל ביעילות נתונים עקביים שנתגלו בחקירה.
- רישום: נועד על מנת שיהיה ניתן לשחזר בקלות את כל הפעולות שנעשו. כל הפקודות נרשמות בדיוק כפי שהן בוצעו במערכת.

תהליך חקירת המידע:

ניתן לחלץ מידע מהזיכרון הראשי באחת מאפשרויות החיבור Volatility (כל חיבור רשת פעיל או שנסגר לאחרונה). בנוסף, ניתן להשתמש בשאלות WHOIS על מנת לצמצם את חיבורי הרשת. כנראה שנצטרך לחזור על התהליך כדי לצמצם עוד יותר את התוצאות ולמרות שיש הרבה כלי חקירה שונים, היכולת לחקור כדי לענות בצורה חד משמעית על שאלות זה הרבה יותר חשוב.

זיהוי חיבור רשת זדוני אפשרי על ידי חקירת כמה פרמטרים:

- מי בעל מערכת ההפעלה.
- ניתוח היסטוריית הגלישה של המשתמש (לזיהוי תדירות או כתובות IP).
- חקירת יומני הרשת שלוכדים תעבורה יוצאת.

תוכנות זדוניות בדרך כלל מתקשרות עם גורם חיצוני במסגרת זמן מסוימת, או במרווחי זמן ספציפיים ובדרך כלל באותו גודל חבילה. תמיד נחפש תוכנית שמתחילה את חיבור הרשת ושאינה חלק מתוכנית מהימנה כלשהי. כל צעד בדרך, הוא איסוף מידע נוסף לבניית תיק חקירה ייסודי וכל אחד מהשלבים הללו כוללים גם חותמות זמן.

התקדמות חקירת הזיכרון:

- המידע מורכב בדרך כלל **מכתובת IP , מזהה תהליך ושם תהליך משויך**. בנתונים אלה תמיד קיימות חותמות זמן וזה מאפשר לבצע חקירה לפי זמנים ולהתאים מול המידע שנמצא בכונן הקשיח. חשוב לדעת שישנן תוכנות היכולות לשנות את חותמת הזמן על מנת להפיל חקירה.
- אחד היתרונות של ביצוע ניתוח זיכרון הוא שתוכנות זדוניות עדיין לא מבצעות פעולות כנגד תוכנות פורנזיות בתוך זיכרון RAM. **הערה:** תנועת רשת יכולה לשמור פלט פקודה בתבנית dot. שיכול להיקרא על ידי **AUTOPSY** על מנת להציג נראות גרפית של יחסי ה-PID ל-PPID שמאפשרת לעקוב אחר מידע כמו האם זוהה קובץ משתמש בכונן, ו/או האם התוכנה הזדונית נפרדת ומוגבלת (בניגוד לקוד המזריק את עצמו לתהליך פועל).

לאחר מכן, אפשר להמשיך בחקירה:

- אם התוכנה הזדונית עצמאית, אפשר לחלץ אותה מהכונן הקשיח באמצעות תוכנה פורנזית. ניתן גם לסרוק תהליך באמצעות סורקים המסוגלים לחלץ תוכניות מוצפנות.
- בחינת קבצי ה-PCAP עבור היישום או התהליך ולצפות ב-packets של TCP./IP וב-UDP.
- מאחר וניתן לעשות מניפולציות על חותמות זמן מהכונן, צריך לבדוק התאמה באמצעות חותמת הזמן שחולצה מהזיכרון (אחת הדרכים הטובות ביותר לזהות חותמת זמן של תוכנה זדונית).
- במידה ויש לנו כונן קשיח שלא הייתה בו לכידת זיכרון RAM, עדיין ניתן לעבוד עם כונן כזה בעזרת VMware.
- לוודא שבכונן המשוכפל מותקן Live View.
- נשתמש ב- VFC כדי ליצור ויזואליה של VMware.
- נעדיף תמיד לעבוד ב- VMware כדי לפתוח קובץ ולפעול על המערכת.
- אם המערכת מוגנת באמצעות סיסמה, ל-VFC יש יכולת לעקוף את תהליך האימות.
- במיקום שבו מאוחסנת תמונת VMware מעתיקים את הקובץ עם הסיומת vmem. (virtual memory).

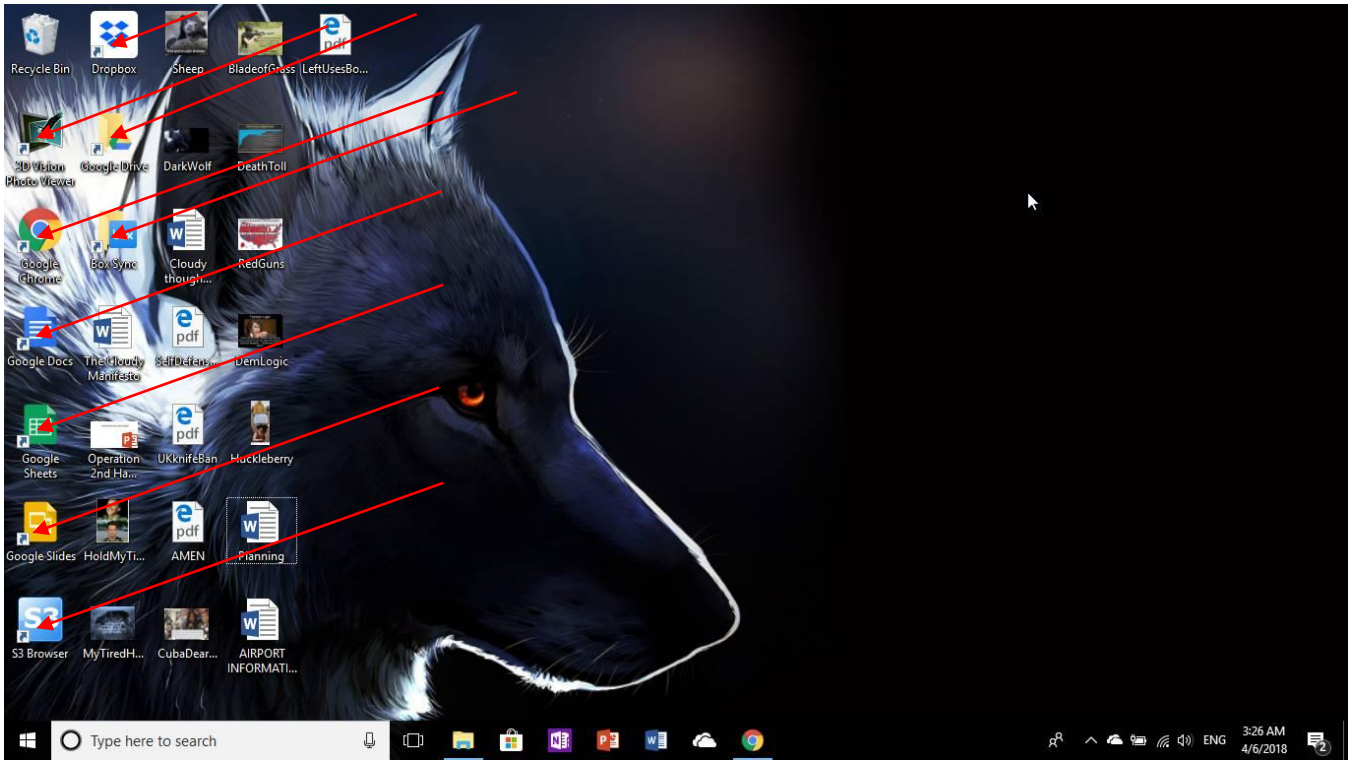
תוכנות זדוניות מסוימות מסוגלות לשרוד באתחול של מחשב, לכן רצוי לתת למחשב לפעול לזמן מסוים, למקרה שהתוכנה הזדונית מעכבת את זמן ההפעלה שלו. Sniffers כמו Wireshark או tcpdump צריכים לרוץ כדי ללכוד את תעבורת הרשת שבודקים (יש אפשרות לבחור בין תהליך אחד שמעניין אותנו, או לחלץ את כל הקבצים שנמצאו) ובעזרתם נוכל למצוא מידע כמו תוכן דואר אלקטרוני, צ'אטים וקבצים. בנוסף, אפשר גם להכניס את הקבצים לתיקייה ואז להשתמש בסורקי אנטי-וירוס שונים כדי לסרוק אותה למציאת תוכנות זדוניות.

זיכרון ה-RAM מכיל כל פיסת מידע. כל קלט או פלט יעבור בזיכרון במערכת מחשב שפועלת:

- **צפיה בחיבורי רשת:** המידע החשוב ביותר מכיל את כתובות ה-IP המרוחקות ומספר פורטי היציאה המשמשים בחיבורי רשת. אפשר לבדוק את הנתונים באמצעות הפקודה "netstat" ב-"Wireshark", המזהה את היעד המרוחק שאליו מתקשרת התוכנה הזדונית שיכולה גם לעזור בזיהוי סוג התעבורה (HTTP, SMTP, FTP) , או יציאה לא ידועה שזוהתה.
- **תהליכי ריצה של זיכרון RAM (זיכרון גישה אקראי):** רשימת משימות של תוכניות פועלות יכולה לספק לחוקרים מידע על אופן השימוש במערכת:
  1. נבדוק את הממשק הגרפי (GUI).
  2. נבדוק את שולחן העבודה על ידי "מנהל המשימות" בשביל לקבל מידע לגבי התוכניות שפועלות. זה נותן מושג כלשהו אם תוכנה זדונית פועלת במערכת, מאחר וכל תהליך לא ידוע יכול להיות תוכנה זדונית שצריכה להיחקר.
- **אישורי משתמש:** שם המשתמש וסיסמה כדי להיכנס ל-EMAIL, לרשתות חברתיות, חשבון בנק ואפילו ל-WIFI של הבית. לכן, אפשר לבדוק בבראוזר ו\או לבדוק במיקום שבו אישורי היוזר נשמרים (לצמיתות או זמנית).
- בשביל לחלץ נתוני יוזר מהזיכרון נשתמש בכלי פורנזיקה שונים כדי לעקוף את האבטחה ולגשת לזיכרון וגם לעקוף קודי סיסמה של המשתמש או נעילת תבניות באם יש.
- נמצאו מסמכים המוגנים ע"י **IRM** (Information Rights Management) אשר מגן על קבצים מפני העתקה, צפייה, הדפסה, העברה, מחיקה ועריכה בלתי מורשים.

שאלות שעלו בזמן התקדמות החקירה ותשובות:

- **מהי מערכת ההפעלה וארכיטקטורת המעבד?**
  - Microsoft Windows NT 6.2.9200.0
  - Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz
- **מי היה המשתמש העיקרי של המחשב?** Jim cloud
- **מי היה המשתמש העיקרי של הדוא"ל ואיזה?** Jim cloud עם jimcloudy1@gmail.com
- **מי היה המשתמש העיקרי של שירותי הענן ואיזה?** Jim cloud עם Microsoft Edge ו-Google Chrome.
- **מהו קובץ LNK שנמצא בדיסק של החשוד?** קובץ shortcuts שמכיל את סוג הקיצור, מיקום (תיקייה, כונן או התקן אחר), שם הקובץ ואת התוכנית שפותחת את הקובץ. הקיצור דרך מזוהה ע"י סימון קטן של חץ הנמצא בצד שמאל תחתון באייקון של תוכנית המקור. **(הערה**: אם קיבלנו קובץ LNK כקובץ מצורף למייל, יש לשים לב מאחר וככל הנראה מדובר בווירוס ולכן יש למחוק אותו). דוגמה לקבצי LNK מצילום מסך מהמחשב של החשוד:



- **ל- Windows יש חותמות זמן שונות בקבצים, מה הן?**

1. חותמת זמן גלובלית - הזמן הזה מאותחל באפס ומקודם בתחילת כל פעילות.
2. חותמת זמן של קבצים - מראה תאריך ושעה בו נוצרו\שונו קבצים ובנוסף התאריך ושעה בהם נפתחו לאחרונה.
   - זמן גישה אחרונה
   - זמן שינוי אחרון
   - זמן שינוי סטטוס אחרון
3. חותמת זמן בפרוטוקול תקשורת - לדוגמה ב-ICMP קיימת הודעת שליחת חותמת זמן והודעת תשובת חותמת זמן.

ממצאים מחקירת הדיסק:

מסמכים המעידים על מחשבות ותכנון ביצוע תקיפה של החשוד:

Cloudy thoughts (4apr).docx

- MD5: f8c2bc733c109a88405dfd13b47d0690
- מיקום: C:\Users\jcloudy\Desktop\
- שונה: 22:39:30 2018-04-04
- גישה: 22:39:30 04-04-2018
- נוצר: 22:39:29 2018-04-04
- שונה: 22:39:41 2018-04-04
- LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jcloudy\Desktop\Cloudy thoughts (4apr).docx

  I don't know if this plan will work. Plans never survive first contact. I don't expect to fail, but there are so many possibilities. But now the weather. Its going to snow, and the winds will be strong. No problem for the attack, but if my flight is delayed or cancelled, that might prove to be a problem.
  I'm stressed and writing used to help me calm down. It seems to be working. Im leaving a lot behind, and the weight of this responsibility is almost too much to handle. I wont stop now, though. Even if I'm killed at the site, I know that what im doing is just and right. Freedom requires sacrifice. If I must be that lamb, then I walk to my slaughter freely of my own accord.
  I am saving everything to the cloud on several accounts. I don't want my words mixed up, and I don't want my thoughts deleted. I want my family to understand why I did this. I think they will keep my secret if I am successful and leave the country without problems. The only record will remain in the cloud and Paul will have the only other keys. My fate will be in God's hands. I pray I have the strength and the luck necessary to persevere. Please let the weather clear!

The Cloudy Manifesto.docx

- MD5: 14c07920ddc81fbd489e61d60e5c9f28
- מיקום: C:\Users\jcloudy\Desktop\
- שונה: 21:35:27 2018-04-01
- גישה: 21:35:27 2018-04-01
- נוצר: 21:35:27 2018-04-01
- שונה: 21:35:39 2018-04-01
- LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jcloudy\Desktop\The Cloudy Manifesto.docx

  What happens when the government can no longer protect you. What happens when you need protection from the government? What happens when you can no longer protect yourself?
  You are responsible for your own safety and protection. You may choose to provide that safety by handing the responsibility over to elected officials and paid public workers. This has worked well for many years, and I have nothing against this system. However, with the increased scrutiny of law enforcement officials comes a shortage in those jobs. Now, your decision to sub-contract your safety may have a negative impact. Response times may increase. Investigations may not get solved. So, again, whose job is it to protect you?
  It's yours. If you choose not to protect yourself, that is YOUR choice. Your choice to be a sheep should not affect other's abilities to protect themselves. Look at Clive Bundy and the now the Snake River Ranchers. Without the

means to protect themselves, they would have been victims of the government. Without the means to protect yourself, you may be a victim of the same, or of your fellow man.

This may be the most absurd statement yet. This is like saying, when the speeding driver sees that everyone else is doing the speed limit, he will slow down. Well no, he's in a hurry and you are in his way. Just like when a shooter wants to do something...he does. The laws won't stop him, and neither will disarming yourself.

So are we really concerned about what is killing us? Why not outlaw unhealthy food? Oh, its our right to eat what we want? You don't say?!

If only it were just a "pair" of sheep. Rather than thousands of sheep we really have. You want to protest the police that protect us, then you want to protest the guns that protect us. I don't think many understand that protection is a right. If you get rid of the police and get rid of the guns, then what are you planning to invite in?

Exactly. Is this movement being led on by Russian, and other State-Level internet trolls. Are they hoping we destroy ourselves from within? If so, why?

This is why. They know they can't take us in a fight. Our military is full of people who grew up around guns and are comfortable shooting them. Get rid of that and it erodes a portion of our readiness. Perhaps that gives them enough edge against our young men to win, or to arrive on our shores. Well right now, as you can see from the quote above, they wouldn't consider it. Our insurgency would put those in the middle east to shame. We would organize and hit them hard. After traveling so far they would be spread thin and be easy pickings for our gun-toting Patriots! But, disarm the populace and no matter how tired they are when they arrive, they will have plenty of time to rest up while we hurl rocks and canned goods at them. Or while we hide in our houses and do as they say to avoid annihilation.

So you wanna take my guns?

I'm your Huckleberry. Just how is it you plan to kill me and take it when you protested the police out of business and you are afraid of guns?

This will never stop. Once they outlaw guns, criminals will turn to knives. Then they will try to outlaw those as well. This is happening in the UK now. They already outlawed guns, and now they want to outlaw pocket knives. Now they are going after free speech by convicting a comedian of making a joke when his dog raised his paw to a TV show featuring footage of Hitler. He wasn't saying hitler was good. He was saying wow, look at my evil dog. But the context didn't matter.

So stop saying it worked for the UK. Well if we agreed with everything they did, we wouldn't exist right now, we'd still be a part of them. Something must be done to show that gun-free zones do not work and will never work. So I intend to break the law. Because that's what the criminals will do. No matter your laws, when they decide to act, they will. Drugs have always been illegal, but that doesn't stop people from getting drugs. Speeding is illegal, but people still drive fast. Fraud is illegal, but greed is a strong motivator. So I will be the lone wolf that helps demonstrate to the American Public that laws and signs won't work. Only the ability to protect yourself will work.

The Second Amendment was not "poorly written" it was drafted by the same men who drafted the rest of the Constitution. And no one is complaining about he protections and freedom it gives you. Especially the 1st amendment which allows you to spew your crazy gun-control thoughts.

You will soon see when the blood has been shed and the defenseless bodies stacked high. I will do what I must. No matter who is hurt, the collateral damage will be worth it.

I will be the change. I will be the revolutionary. I will be the history maker. I will fight**. I will be the Lone Wolf.**

Planning.docx

- MD5: 4ef414e469b7830faa2db429fe1321ee
- מיקום: C:\Users\jcloudy\Desktop\
- שונה: 01:30:41 2018-04-04
- גישה: 01:30:41 2018-04-04
- נוצר: 22:16:48 2018-03-29
- שונה: 01:30:49 04.04.2018
- LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jcloudy\Desktop\Planning.docx

Planning

1. Target
    a. Must have good escape route
    b. Preferably near Airport
    c. Must be Gun Free zone.

2. Supplies
    a. Gun (black market)
        i. Norther VA Gun Works 7518 Fullerton Rd # K, Springfield, VA 22153
        ii. NOVA 412 W Broad Street Falls Church, VA 22046
        iii.
    b. Ammo.
        i. 9mm is 1000 for $360
        ii. Kel-Tec Sub 2000 9mm $400.
    c. Latex gloves
    d. Velcro tear away clothing?
    e. Cash

3. Escape
    a. No Extradition countries
        i. Indonesia (Nicer, but more expensive)
        ii. Vietnam
        iii. Can live very well on 100 a day, for 9 years.
    b. Buy tickets for same day
    c. Preferable direct flight
    d. Have suitcase in car.

4. Release
    a. Start writing ideas and thoughts
    b. Save to separate locations for redundancy
    c. Place it in the cloud for remote access
    d. "Press Release" once home free.

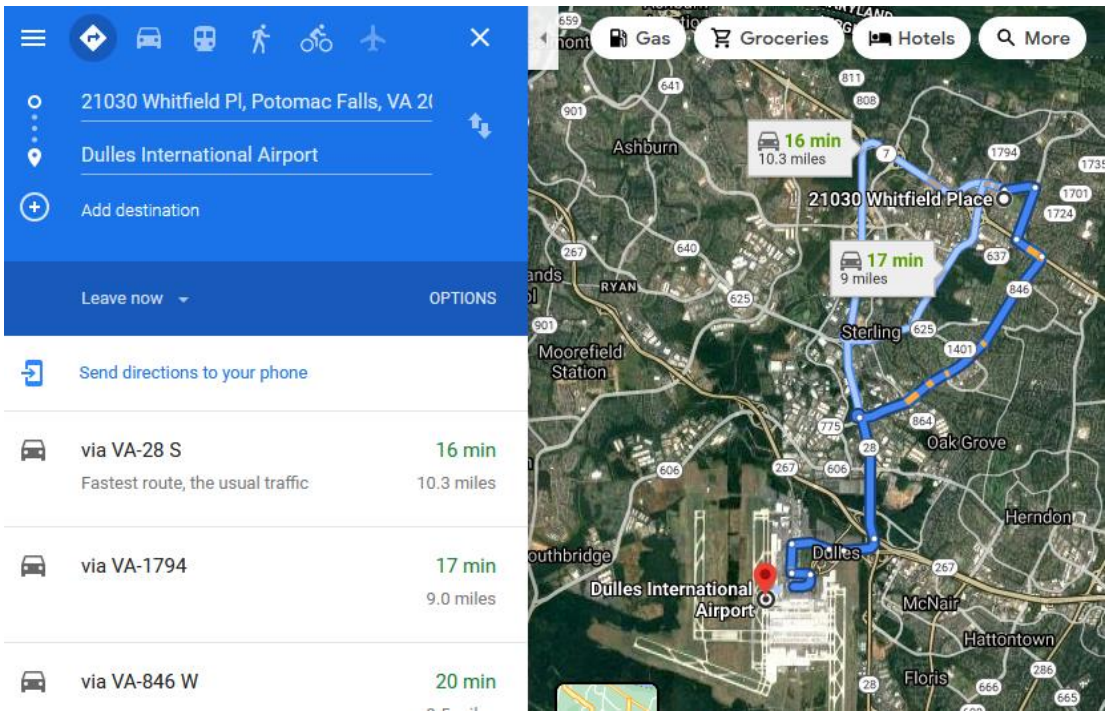
Operation 2nd Hand Smoke.pptx

- MD5: b301fbf4104fb64b566b076c12a5d113
- מיקום: C:\Users\jcloudy\Desktop\
- שונה: 01:11:27 2018-04-04
- גישה: 01:11:27 2018-04-04
- נוצר: 00:56:19 2018-04-04
- שונה: 01:11:53 2018-04-04
- LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jcloudy\Desktop\Operation 2nd Hand Smoke.pptx

נמצאה מצגת Power point עם תוכנית התקיפה של החשוד. במצגת קיימים צילומים של המטרה, מסלול בריחה, מידע על טיסות והמלון ששם תכנן להיות.

AIRPORT INFORMATION.docx

- MD5: 297eec248647f33f887d72328ab56f3c
- מיקום: C:\Users\jcloudy\Desktop\
- שונה: 00:59:32 2018-04-04
- גישה: 00:59:32 2018-04-04
- נוצר: 22:29:57 2018-03-29
- שונה: 00:59:40 2018-04-04
- LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jcloudy\Desktop\AIRPORT INFORMATION.docx



סיכום

בחקירה הפורנזית של הדיסק והזיכרון אשר נלקחו מהמחשב של החשוד נמצאו מסמכים הקושרים אותו ללא עוררין לתכנון הפיגוע - תוכנית תקיפה, נתיב בריחה, כרטיס טיסה ופרטי שדה התעופה שממנו החשוד תכנן לברוח מהמדינה.

התכנון היה לבצע פיגוע ירי המוני בכנס עירייה בהשתתפות סנטורים ואנשי ממשל מקומיים בנושא אלימות בנשק, ביטחון בבתי ספר\בציבור בתאריך 7 לאפריל 2018 בין השעות 12:30 – 14:00 בספרייה הנמצאת ב-Whitfield Place. החשוד תכנן להיכנס לספרייה בזמן הכנס, לבצע את הפיגוע ומיד לאחר מכן לברוח לשדה התעופה בדאלאס ומשם לאינדונזיה, בהתאם לתוכנית הבריחה שנמצאה בחקירה.

לאחר חקירת הדיסקים, אפשר לקבוע כי החשוד פעל לבד ואף נמצא שהוא הצהיר על עצמו שהוא **LONE WOLF**.

קובץ אקסל המכיל עדויות לפעילות של החשוד:

forensics data LONE WOLF 2021.xlsx

קורס: 7735 מגן סייבר אבטחת מידע והגנה על רשתות ארגוניות
מרצה: ליאור ברש
מגיש: רועי טוכבנד ת.ז. 37213816
תאריך: 14.7.21