

THE CYBER KILL CHAIN®

שרשרת תקיפה



Yosi Shavit MBA, CISM - Information Security & Cyber Expert

Cellular: 058-6662242

Mail: yosish@gmail.com , yosish@sviva.gov.il

נושאי הלימוד

הנושאים הנלמדים בקורס זה:



- מיהם התוקפים ומה מטרתם
- מתודולוגיית CYBER KILL CHAIN
- שלבי תקיפה מרכזיים על פי תאוריית לוקהיד.
- איסוף מידע במבט התוקף
- הנדסה חברתית.
- טשטוש עקבות

מיהם התוקפים ומה מטרתם ?



פושעים

אקטיביסטיים

האקרים
פושעים

מתחרים
עסקיים

סייבר
מדינתי

עובד
ממורמר

מטרות התוקפים

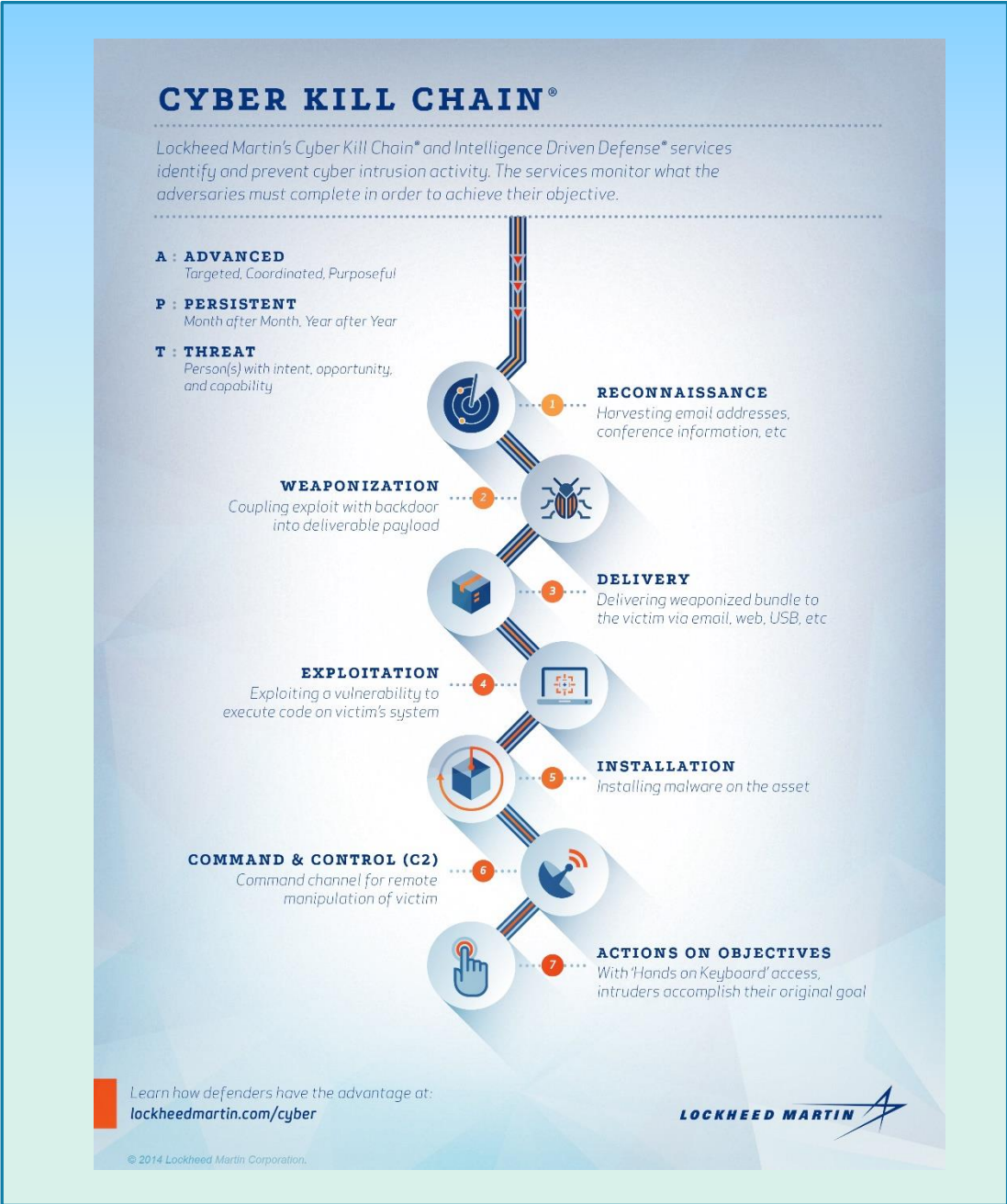
- גרימת נזק מכוון (פוליטיקה, אידיאולוגיה, מתחרים, נקמה)
- גניבה מידע פיננסי (כרטיסי אשראי, מצב חשבון, וכו')
- גניבת כסף – חדירה לחשבון אישי בבנק
- הפללה – ניתן להפליל משהו ברגע שיש גישה למחשב
- ריגול תעשייתי
- מודיעין / ריגול – מעקב אחר הפעולות במדיה הדיגיטלית
- סחיטה – כופרות
- גניבת מידע אישי
- הוכחת יכולת (אגו)
- כריתת מטבע וירטואלי BITCOINS



CYBER KILL CHAIN – רקע הסטורי

- בשנת 2011, חברת לוקהיד מרטין האמריקאית פרסמה מאמר אשר סוקר את התהליך שמבצע יריב מתקדם בעת תקיפה בסייבר על יעדיו.
- סקירה זו נחשבת לאבן דרך משמעותית בחשיבה אודות הגנה בסייבר, ועודדה ארגונים וגופי הגנה רבים לתכנן את הגנתם לפי הצעדים של היריב ולהשיג מודיעין מתאים על כל שלב.





CYBER KILL CHAIN

7 שלבי תקיפה



שלב ראשון – סיור Reconnaissance

איסוף מידע במבט של תוקף

- איסוף מידע של התוקף על היעד הנתקף – מכל מקור אפשרי
- מבצעים סריקת פורטים פתוחים ונקודות חולשה שיכולים להוות מקור לפריצה
- איתור רכיבי אבטחת מידע שקיימים בארגון כמו חומת אש, IPS וכדומה כמו גם מערכות לזיהוי
- איתור מידע על הארגון הנתקף דרך אתר האינטרנט שלו
- איתור מידע באמצעות "הנדסה חברתית"
- איתור מידע ע"י חיטוט בפחי אשפה



דרכים לאיסוף מידע

- ✓ אינטרנט - Google
- ✓ אתר האינטרנט של הארגון
- ✓ רשתות חברתיות – FACEBOOK , LINKEDIN
- ✓ Google hacking
- ✓ הנדסה חברתית
- ✓ Sniffing
- ✓ כלי סריקה
- ✓ הגעה פיסית לאתר הנתקף



דוגמא: השגת פרטי טלפון ומייל באינטרנט



פורטל המבקרים שירות צרכנים חדשות מהעולם חוק סימון תזונתי

פרופיל חברה
 חזון
 יצור ומפעל
 איכות
 נגישות
הנהלה בכירה
 מערך מכירה והפצה
 שאלות ותשובות

הראל חייקין
 מנכ"ל קוקה-קולה ישראל
 דוא"ל - Harel@cocacola.co.il

שלי שמיר קינן
 סמנכ"ל שיווק, קוקה-קולה ישראל
 דוא"ל - ShellySK@cocacola.co.il

אלי בראל
 סמנכ"ל תפעול, קוקה-קולה ישראל
 דוא"ל - EliBa@cocacola.co.il

טלי שפיר-משיח
 סמנכ"ל כספים, קוקה-קולה ישראל
 דוא"ל - TaliS@cocacola.co.il

אביחי גרינברג
 סמנכ"ל איכות וטכנולוגיית מזון, קוקה-קולה ישראל
 דוא"ל - AvichaiG@cocacola.co.il

איה אוברבאום לנמן
 סמנכ"ל משאבי אנוש, קוקה-קולה ישראל
 דוא"ל - AyaUl@cocacola.co.il
 קורות חיים ניתן לשלוח לכתובת: cv@cocacola.co.il

FirstName+__@cocacola.co.il

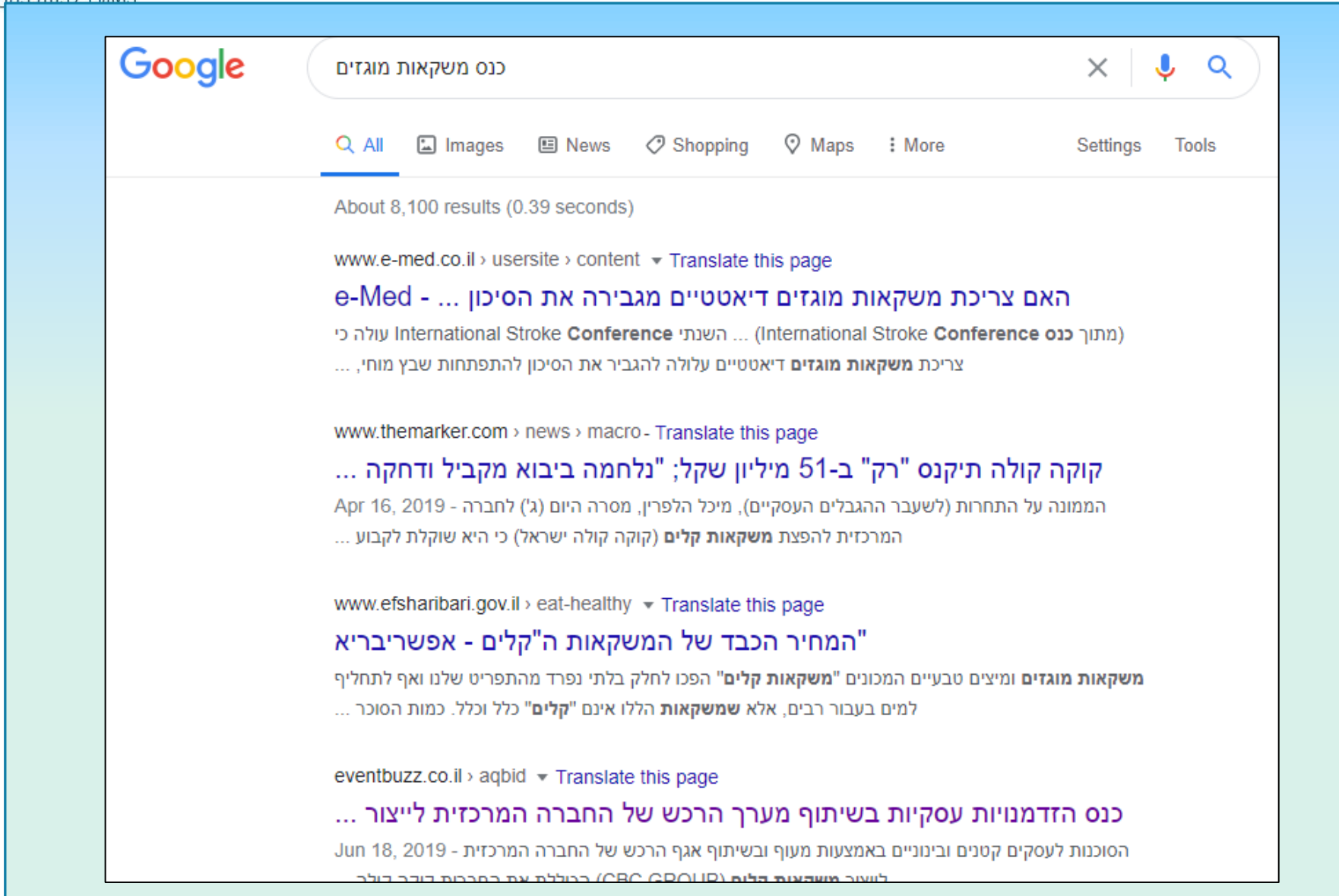
אנו מזמינים אתכם לפנות אלינו בכל שאלה ומבטיחים לתת את המענה הטוב ביותר

הוספת נתונים מרשתות חברתיות

The screenshot shows a LinkedIn profile page. At the top, there is a navigation bar with the LinkedIn logo, a search bar, and icons for Home, My Network, Jobs, and Messaging. Below the navigation bar, there is a header for the profile: "Tech. support- 499\$/month - Engineering support services tailored to your requireme". The main profile section features a blue background with a network diagram. Below this, there are buttons for "Connect", "Message", and "More...". The profile name "VP Quality and Technology at Coca-Cola Israel" and the company name "Coca-Cola Company" are highlighted with a black circle. Below the profile name, it says "Israel · 261 connections · Contact info". The "Highlights" section shows "1 mutual connection" with the text "You and Avichai both know Rami Tshuva". The "Experience" section lists "VP Quality and Technology" at "Coca-Cola Company" from "Jun 2013 – Present · 7 yrs 2 mos" in the "Bnei Brak Area, Israel".



חיפוש פשוט בגוגל – "כנס משקאות מוגזים"



Google

כנס משקאות מוגזים

All Images News Shopping Maps More Settings Tools

About 8,100 results (0.39 seconds)

www.e-med.co.il > usersite > content > Translate this page

האם צריכת משקאות מוגזים דיאטטיים מגבירה את הסיכון ...
e-Med - ...
(מתוך **כנס International Stroke Conference** השנתי ...
International Stroke Conference עולה כי
צריכת **משקאות מוגזים** דיאטטיים עלולה להגביר את הסיכון להתפתחות שבץ מוחי, ...

www.themarker.com > news > macro - Translate this page

קוקה קולה תיקנס "רק" ב-51 מיליון שקל; "נלחמה ביבוא מקביל ודחקה ...
...
Apr 16, 2019 - הממונה על התחרות (לשעבר ההגבלים העסקיים), מיכל הלפרין, מסרה היום (ג') לחברה -
המרכזית להפצת **משקאות קלים** (קוקה קולה ישראל) כי היא שוקלת לקבוע ...

www.efsharibari.gov.il > eat-healthy > Translate this page

"המחיר הכבד של המשקאות ה"קלים" - אפשרי בריא
...
משקאות מוגזים ומיצים טבעיים המכונים "**משקאות קלים**" הפכו לחלק בלתי נפרד מהתפריט שלנו ואף לתחליף
למים בעבור רבים, אלא ש**משקאות הללו** אינם "קלים" כלל וכלל. כמות הסוכר ...

eventbuzz.co.il > aqbid > Translate this page

כנס הזדמנויות עסקיות בשיתוף מערך הרכש של החברה המרכזית לייצור ...
...
Jun 18, 2019 - הסוכנות לעסקים קטנים ובינוניים באמצעות מעוף ובשיתוף אגף הרכש של החברה המרכזית -
לשעבר **משקאות קלים** (CFC GROUP) כוללת את חברות הרכש שלה

<https://eventbuzz.co.il/lp/event/aqbid>



CBC GROUP | מעוף | משרד הכלכלה והתעשייה
הסוכנות לעסקים קטנים ובינוניים

רוצים להיות ספקים של החברה המרכזית לייצור משקאות קלים?

SAVE THE DATE
18.06.19

סליה אירועים, המרכבה 40, חולון
www.maof3.co.il

BDO | ANS | IBBIS | müller | Coca-Cola | פריסה | טרה | Carlsberg | נבועות

כנס הזדמנויות עסקיות בשיתוף מערך הרכש של החברה המרכזית לייצור משקאות קלים

התחלה: 18.06.2019 09:30

מיקום: סליה אירועים- המרכבה 40, חולון (חנייה בחניון התת קרקעי)

להגדלת אמינות

מחפש דמות "משמעותית" בכנס

מאות בעלי עסקים וספקים השתתפו בכנס הזדמנויות עסקיות עם ענקית המשקאות קוקה-קולה

מערכת 'חדשות ישראל' · יוני 26, 2019

הסוכנות לעסקים קטנים ובינוניים במשרד הכלכלה באמצעות מערך מעוף מרחב מרכז, קיימו השבוע (18/6), כנס הזדמנויות עסקיות לקידום רכש מקומי בשיתוף החברה המרכזית לייצור משקאות קלים CBC GROUP. רן קיויתי, מנהל הסוכנות לעסקים קטנים ובינוניים: "נמשיך לפעול להעמקת הרכש של חברות בינלאומיות מעסקים מקומיים".

מאות בעלי עסקים מאזור גוש דן הגיעו השבוע לכנס הרכש הגדול עם ענקית המשקאות הבינלאומית CBC GROUP. הכנס התקיים כחלק מפעולות משרד הכלכלה והסוכנות לעסקים קטנים ובינוניים באמצעות מעוף, לפיתוח כלכלי באזור. בכנס נחשפו מאות העסקים למערך הרכש של החברה ולמדו על תחומי הרכש המבוקשים והתחומים הרלוונטיים לספקים מקומיים.

רן קיויתי מנהל הסוכנות לעסקים קטנים ובינוניים בירך את המשתתפים ואמר: "עסקים קטנים ובינוניים הם מנוע הצמיחה של המשק וזה אינטרס לאומי עבורנו לפעול לחיזוק העסקים ולסייע בחיבורים". כמו-כן, קיויתי סיפר למשתתפים על פעילות הסוכנות לעסקים קטנים ובינוניים, על פעילותיה במרחבי העסקים והיזמות, והפעולות השונות שהסוכנות לעסקים קטנים ובינוניים מבצעת מרמת הנגישות, לאנשים עם מוגבלויות דרך קורסים אינטרנטיים ועד ליווי יעוץ עסקי.



אורי הכהן, מנהל מעוף מרכז. צילום: אפרת סער

סמנכ"ל הרכש CBC GROUP, מר אורן חאיק, בירך על קיום האירוע ועודד את בעלי העסקים להכיר אישית את אנשי הרכש הרלוונטיים, ליצור קשרים והזדמנויות כלכליות לעתיד: "פגשתי כאן היום עסקים רבים בעלי פוטנציאל להפוך לספקים שלנו. אני קורא לכם, תשתמשו במידע ובכלים שקיבלתם היום ותהיו יד ביד חלק מההצלחה".

החברה המרכזית לייצור משקאות קלים CBC GROUP - היא בעלת המותגים קוקה קולה, נביעות, טרה, קרלסברג, פריגט ועוד.

אורי הכהן, מנכ"ל מעוף מרכז הוסיף בפני המשתתפים: "הגעתם לכנס לטובת שתי מטרות: חיבור למנועי הרכש של CBC GROUP ומינוח למנועי הרכש שלכם ושלכם".



מה יש לי עד כה לצורך ביצוע הכנסת הקוד הזדוני?

1. כתובות מייל של בכירים בארגון המופיעות באתר:

✓ הראל חייקין מנכ"ל קוקה קולה : harel@cocacola.co.il


✓ אביחי גרינברג – סמנכ"ל איכות וטכנולוגיות avichaig@cocacola.co.il

2. כתובת "השולח" – איש קשר מהכנס : מר אורי הכהן – מנהל מעוף מרכז משרד הכלכלה

3. "אליבי" למשלוח הקוד – כנס משקאות מוגזים .

4. יצירת קובץ PDF (או כל קובץ אחר) המכיל את הקוד הזדוני

דרך נוספת לאיסוף מידע Google Hacking

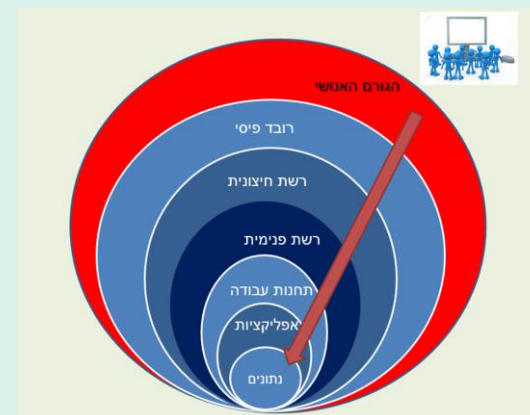


The screenshot shows the Google Hacking Database interface. At the top, it says "GOOGLE HACKING-DATABASE" and "Welcome to the google hacking database". Below that, it says "We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!". There is a search bar with a dropdown menu set to "All" and a "Search" button. Below the search bar, there is a section titled "Latest Google Hacking Entries" with a table of results.

Date	Title	Category
2013-11-25	site:github.com inurl:sftp-config.json intext:/wp-...	Files containing passwords
2013-11-25	site:github.com inurl:sftp-config.json	Files containing passwords
2013-11-25	inurl:github.com intext:sftp-conf.json +intext:/wp-...	Files containing juicy info
2013-11-25	allinurl:"owa/auth/logon.aspx" -google -...	Pages containing login portals

הנדסה חברתית – SOCIAL ENGINEERING

- הנדסה חברתית היא סוג של מתקפה פסיכולוגית התוקף מוליך אתכם שולל לבצע משהו שהוא מעוניין שתבצעו.
- האקרים למדו ששימוש בטכניקה זו באינטרנט הוא יעיל מאוד ויכול לשמש לתקיפת מיליוני אנשים.





הנדסה חברתית - סוגים של התקפות

בדוגמא שלנו: שילוב של השלושה

- פישנינג (Phishing)
- התקפות ממוקדות (Spear Attacks)
- התחזות (Impersonation)
- גישה פיזית (Piggybacking, Tailgating)
- הצצה (Shoulder surfing)
- חיפוש בפחי זבל (Dumpster diving)
- שימוש בתוכנות מזויפות (Fake software)



Piggybacking, Tailgating

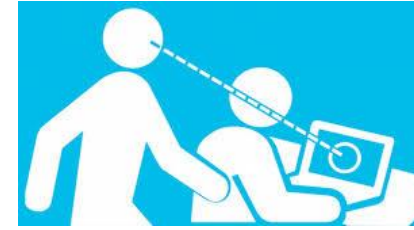
Piggybacking



דוגמאות

- ❑ הכנסת אורחים
- ❑ דלת מסתובבת
- ❑ הצמדות לאדם נכנס
- ❑ עובד תחזוקה
- ❑ נכנס עם 2 כוסות קפה

Shoulder Surfing





"הארגזים היו מונחים על המדרכה עם ערימות של מסמכים פתוחים בצורה כזו שכל אחד כמוני יכול היה לקחת", סיפרה בתיה בונה, שהבחינה בניירות הרבים בשעה שעברה במקום. באחד המסמכים נכתב על מישהו שיש לו אסטמה קלה, רשרוש בלב ועבר אקו-דופלר, במקום אחר כתוב על מישהו שלאבא שלו רקע משפחתי של סרטן. אם מישהו היה מעיז לשים את התיק הרפואי שלי באמצע הרחוב הייתי הולכת עם זה עד הסוף".

מרבית הטפסים שנזרקו הכילו בדיקות רפואיות לצורך הוצאת כרטיסי שחקן לחברים בליגה למקומות עבודה. חומרת החשיפה של הטפסים לעיני כל עובר ושוב אינה רק בפרטים הרפואיים שבהם (אשר האזרח הממוצע לא יבין מהם הרבה), אלא בעיקר בעובדה שהופיעו בהם מאות שמות פרטיים ושמות משפחה, תאריכי לידה, כתובות, מספרי תעודת זהות ופרטים אישיים נוספים, אשר עלולים לשמש נוכלים ואף גורמים עויינים. בנוסף, מופיעים חלק מהשמות בהקשרים של חשבונות בנק.



המסמכים בזבל. הבדיקות הרפואיות במרכז ת"א (צילום: עופר עמרם)



זורקים את הסודיות הרפואית לזבל

מאות מסמכים, ובהם פרטים אישיים ותוצאות בדיקות רפואיות של אזרחים, נמצאו בארגזים זרוקים מול בניין ההסתדרות בתל אביב והגיע לידי ynet. ראש הלשכה לאתיקה בהסתדרות הרפואית: "תיעוד רפואי אמור להיות סודי וחסוי והרופא שמנהל אותו צריך להפעיל מאמץ סביר וכנה לשמור עליו ככזה"



מיטל יסעור-בית אור

מי השליך לפח הזבל מסמכים ובהם פרטים רפואיים ואישיים של אזרחים? אזרחים שעברו אתמול (ג') על המדרכה הצפונית של רחוב ארלוזורוב בתל-אביב, ליד בניין ההסתדרות, יכלו להבחין בארגזים מלאים במסמכים, אשר במקום להיגרס כמקובל, הונחו ליד פחי הזבל. המסמכים כללו בין היתר תוצאות בדיקות ארגומטריה (ניטור הלב במאמץ) לצד שאלונים רפואיים של הנבדקים.

קפיצה של POP-UP למסך שאמור לנו שהמחשב שלנו נגוע בוירוס או תכנה זדונית ועלינו לנקות
ההודעה מציעה תכנה חינמית לסריקת המחשב ולניקויו
ההודעה היא FAKE והתכנה המנקה היא זו ששותלת את הקוד הזדוני במחשב, או שואבת פרטים
אישיים

קפטן אינטרנט | תוכנות

הורדתם את CCleaner בחודש האחרון? קיבלתם מתנה לא רצויה

האקרים הצליחו להחדיר תוכנה זדונית לעדכון של תוכנת ניקוי המחשב הפופולרית; הגרסה הנגועה
זכתה ל-2.27 מיליון הורדות

שלב שני – בניית אמצעי תקיפה – Weaponization

בשלב זה התוקף בונה את אמצעי התקיפה על מנת לנצל חולשה קיימת

במילים מקצועיות: בניית ה-EXPLOIT לניצול ה-Vulnerability

ניתן להעזר ב :

- ❖ ניצול חולשות ידועות במערכות הפעלה, דפדפנים וכדומה
- ❖ בניית מוטציה לקוד זדוני / וירוס קיים
- ❖ ניצול כלי תקיפה קיימים (KAU LINUX)
- ❖ כתיבת קוד זדוני לביצוע משימה ייעודית.

שלב שלישי – משלוח ליעד Delivery



בשלב זה התוקף שולח את אמצעי התקיפה שבנה ליעד

ניתן להעזר ב :

- ❖ מיילים
- ❖ משלוח קובץ זדוני
- ❖ שליחת לינק לאתר שנפרץ
- ❖ פיזור DOK באתר הנתקף
- ❖ העברה דרך פורטים פתוחים או דרכי גישה פתוחים אחרים (FTP)

Source: <https://www.pinterest.com/pin/2251868541098687/>

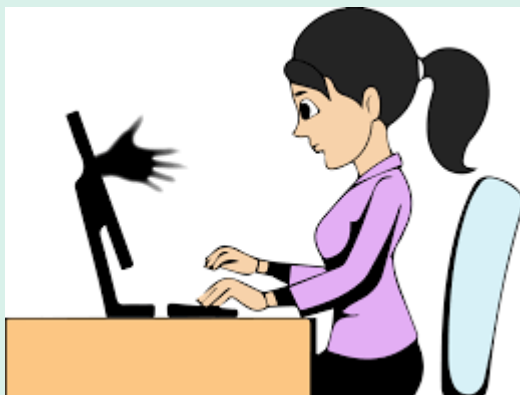
שלב רביעי – ניצול חולשה EXPLOITATION



בשלב זה התוקף **מפעיל** את הקוד שהעביר למחשב הקורבן בשלב הקודם

ניתן להפעיל בדרכים הבאות:

- ❑ הפעלת POWER SHELL
- ❑ ניצול הגיזבים שרצים במחשב באמצעות ה-SCHEDULER של מיקרוסופט שנמצא בכל מחשב
- ❑ ניצול מנגנונים של מיקרוסופט להרצת תהליכים במחשב (PSEXEC)

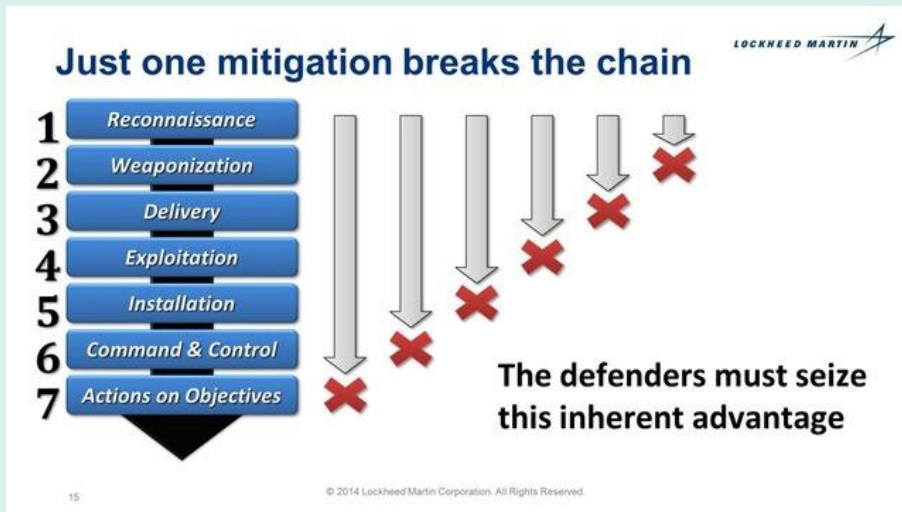


שלב חמישי – התקנה Installation

בשלב הקודם הועברה הנוזקה אל הקורבן ע"י ניצול החולשה .

בשלב זה מופעלת הנוזקה, אם זה קובץ ריצה מריצים אותו והוא מתחיל להפעיל את הרכיבים שנכתבו בתכנה למשל:

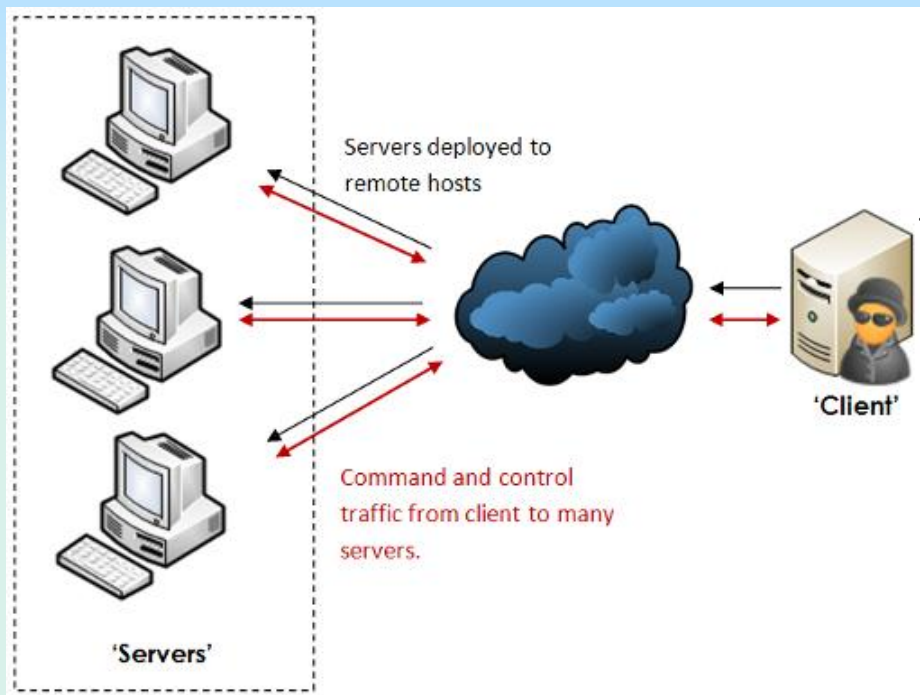
- שינוי רישום בבסיס הנתונים של מערכת ההפעלה
- פתיחת תקשורת ממחשב הקורבן לעולם
- התקנת שירות (SERVICE) במחשב הקורבן כך שגם הם יכבו את המחשב וידליקו אותו – הנוזקה תעלה כשירות



Source: <https://docs.sucuri.net/website-firewall/website-firewall/intrusion-kill-chain/>

שלב שישי – שליטה מרחוק

C&C – Command & Control



❑ ביסוס אחיזה

❑ ישנה תקשורת רציפה בין התוקף לקורבן

❑ גם אם הקורבן כיבה והדליק מחשב התקשורת בינו לבין התוקף תחזור

❑ התוקף שולט במחשב הקורבן ויכול להריץ ממנו פקודות שונות

❑ התוקף יכול לגרום למחשב הקורבן לתקוף יעדים עבורו (DDOS)

❑ מכאן התוקף יכול לבצע LATERAL MOVEMENT

Source: <https://www.hackercoolmagazine.com/hacking-windows-poisonivy-buffer-overflow-exploit/>

שלב שביעי – הרצת פקודות ופעילות



- בשלב זה התוקף עושה כל העולה על רוחו במחשב הקורבן
- התוקף שולט במחשב הקורבן ויכול להריץ ממנו פקודות שונות
- התוקף יכול לגרום למחשב הקורבן לתקוף יעדים עבורו (DDOS)
- מכאן התוקף יכול לבצע LATERAL MOVEMENT
- התוקף יכול להתקין SNIFFER
- התוקף יכול לחפש את בסיסי הנתונים (ע"י חיפוש הפרוטוקולים של בסיסי הנתונים)
- יכול להשיג משתמשים וסיסמאות נוספות
- יכול לדלג לרשתות אחרות כוללת רשת ה-OT
- יכול לחפש את מערכות המיחשוב המדברות עם מערכות ייצור (ע"י חיפוש פרוטוקול של MODBUS)

טשטוש עקבות

- מחיקת קבצי לוג
- מחיקת היסטוריית command line
- שימוש ב- Rootkit (תכנה המאפשרת גישה מתמשכת ובעלת הרשאות למחשב, ובה בעת מסתירה את נוכחותה)



