המשרד להגנת הסביבה

סייבר בתעשייה
המשרד להגנת הסביבה

התאחדות התעשיינים בישראל

שרשרת תקיפה

THE CYBER KILL CHAIN®

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com yosish@sviva.gov.il

התאחדות התעשיינים בישראל

נושאי הלימוד

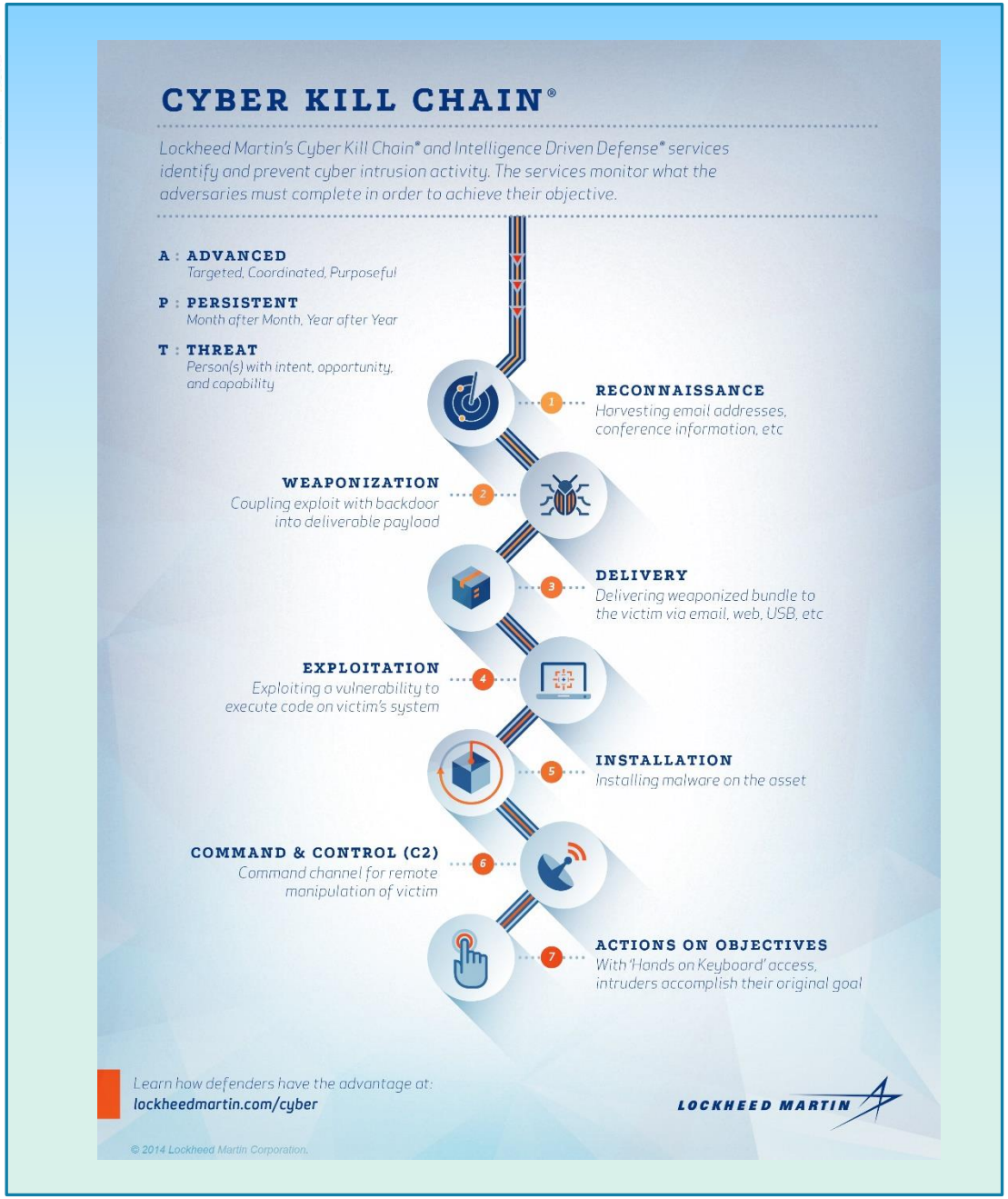
הנושאים הנלמדים בקורס זה:

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

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.

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com yosish@sviva.gov.il



CYBER KILL CHAIN

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com yosish@sviva.gov.il

7 שלבי תקיפה

Reconnaissance - סיור	מחקר, זיהוי והשגת מידע חיצוני על היעד המבוקש
בניית אמצעי תקיפה Weaponization	הצמדה של סוס טרויאני לקוד המנצל חולשה (exploit) ביחד עם אמצעי העברה אשר מתאימים ליעד הנתקף
Delivery - משלוח ליעד	משלוח אמצעי התקיפה שנבנה בשלב הקודם אל הארגון הנתקף
ניצול החולשה ביעד Exploitation	לאחר משלוח כלי התקיפה לרשת הארגון הנתקף, מתבצעת הפעלה של אמצעי התקיפה באופן המאפשר הרצת קוד שאותו תכנן התוקף
Installation – התקנה	בשלב זה מותקן כלי על גבי מחשב בארגון הנתקף ומאפשר לתוקף תקשורת מרחוק למול הכלי המותקן על המחשב - Remote Access Tool
שליטה ובקרה Control & Command	תקשורת רציפה בין התוקף לבין הכלים שלו המותקנים במחשב ברשת הנתקף
פעילות ביעד התקיפה Actions on Objective	התוקף יבחר, מה ברצונו לעשות: לחקור את רשת היעד בכדי להבין לאן הוא מעוניין להגיע, לגנוב מידע, לפגוע ברשת היעד ובתהליכים בה היא תומכת ועוד

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com yosish@sviva.gov.il

התאחדות התעשיינים בישראל

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

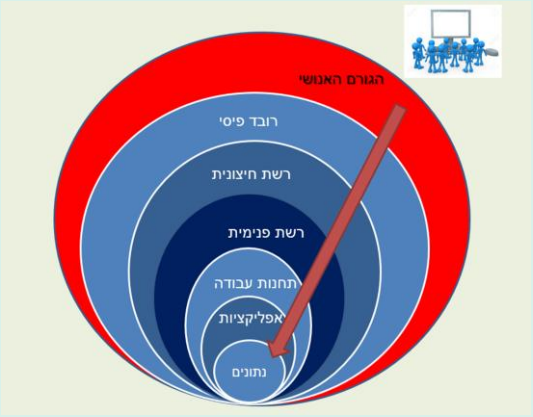
Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com yosish@sviva.gov.il

דרך נוספת לאיסוף מידע
Google Hacking

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com yosish@sviva.gov.il

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.



Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com yosish@sviva.gov.il

הנדסה חברתית - סוגים של התקפות

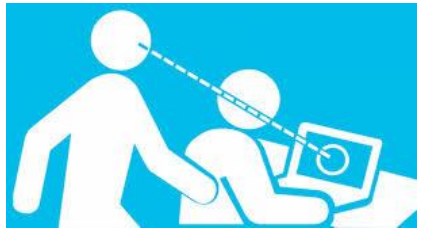
- פישינג (Phishing)
- התקפות ממוקדות (Spear Attacks)
- התחזות (Impersonation)
- גישה פיזית (Piggybacking, Tailgating)
- הצצה (Shoulder surfing)
- חיפוש בפחי זבל (Dumpster diving)
- שימוש בתוכנות מזויפות (Fake software)

Piggybacking, Tailgating

דוגמאות

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

Shoulder Surfing



Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com yosish@sviva.gov.il

Dumpster Diving

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 ארלוזרוב 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.

"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)

Fake software

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

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com yosish@sviva.gov.il

שלב שני – בניית אמצעי תקיפה – Weaponization

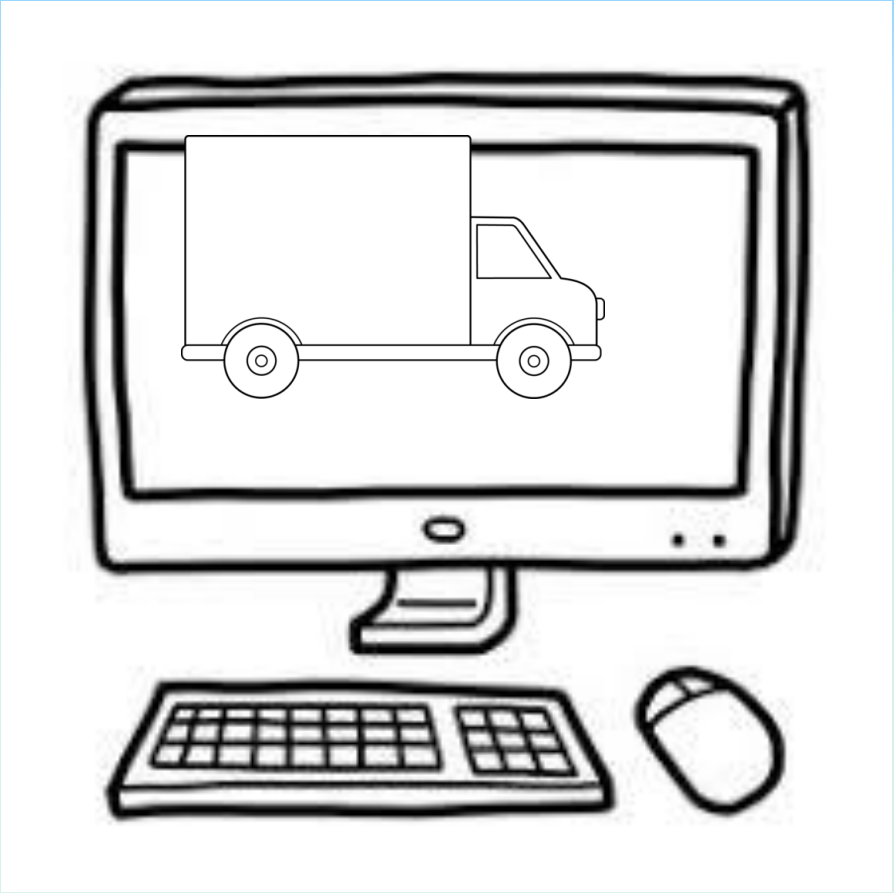
בשלב זה התוקף בונה את אמצעי התקיפה על מנת לנצל חולשה קיימת

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 (KALI LINUX)
- כתיבת קוד זדוני לביצוע משימה ייעודית.

שלב שלישי – משלוח ליעד Delivery



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

בשלב זה התוקף שולח את אמצעי התקיפה שבנה ליעד

ניתן להעזר ב :

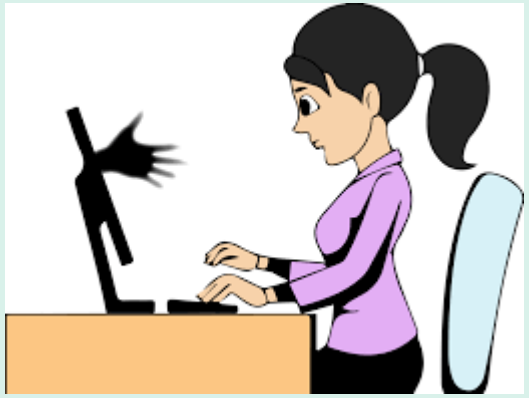
- מיילים
- משלוח קובץ זדוני
- שליחת לינק לאתר שנפרץ
- פיזור DOK באתר הנתקף
- העברה דרך פורטים פתוחים או דרכי גישה פתוחים אחרים (FTP)

שלב רביעי – ניצול חולשה EXPLOTATION

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

ניתן להפעיל בדרכים הבאות:

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

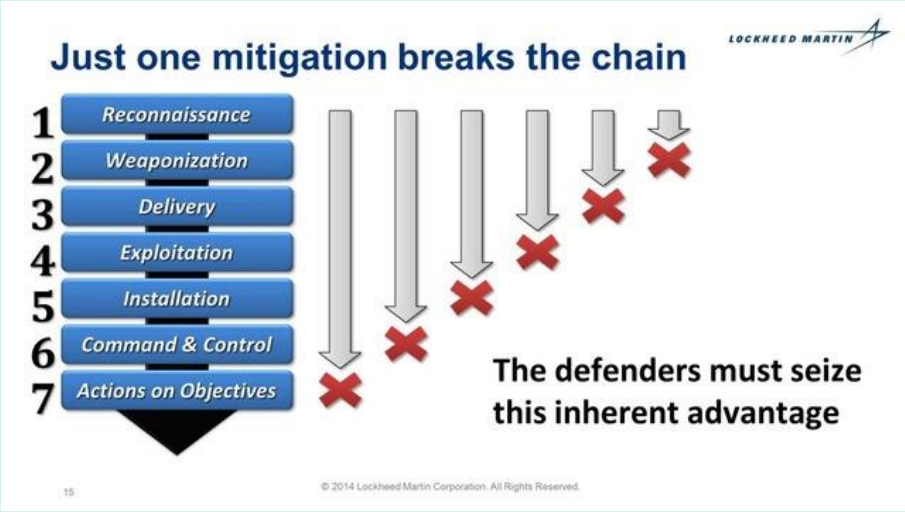


שלב חמישי – התקנה Installation

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:

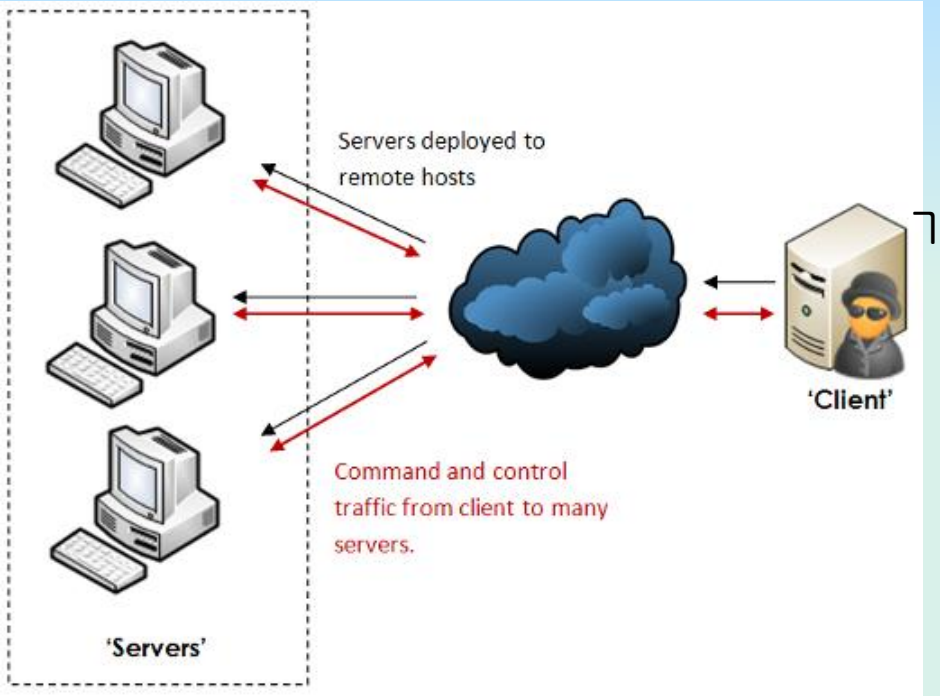
- שינוי רישום בבסיס הנתונים של מערכת ההפעלה
- פתיחת תקשורת ממחשב הקורבן לעולם
- התקנת שירות (SERVICE) במחשב הקורבן כך שגם הם יכבו את המחשב וידליקו אותו – הנוזקה תעלה כשירות
-



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)

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com yosish@sviva.gov.il

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com yosish@sviva.gov.il