

SOC – מטלת גמר

שקד אוריאל ברמי – 213164379

CSPP86

מדריכה – שקד שילו

תאריך ההגשה: 8/5/24



3.....	אירוע 1
3.....	הסברת הזיהוי בלוג
4.....	דעתי על האירוע, תקין?, יש צורך בהרחבת החקירה?
5.....	מה החקירה שהייתי מבצע?
6.....	באיזה שלב בCyber Kill Chain מדובר בעצם?
7.....	איזה טכניקה או טקטיקה מדובר מתוך הMITRE
8.....	אירוע 2
8.....	לחקור את המייל, האם מדובר במייל פשינג?
10.....	סיכום של מה חקרנו ואיך הגעתי למסקנה שלי
10.....	במידה ומדובר במייל פשינג איזה פעולות הייתי מבצע
10.....	על איזה שלב בCyber Kill Chain מדובר
11.....	צינו איזה טכניקה או טקטיקה מדובר מתוך הMITRE
12.....	אירוע 3
12.....	הסבר על החוק, ומה הוא מחפש
12.....	פירוט מהלך החקירה, שאלות שעולות ופירוט
13.....	מה דעתי, האם מדובר באירוע אמת או שווא, ואיך הייתי מטפל באירוע
13.....	באיזה שלב בCyber Kill Chain מדובר
14.....	בנוסף - באיזה טכניקה או טקטיקה מדובר מתוך הMITRE

אירוע 1

קיבלנו קובץ ובו לוג, כעת נפתח אותו וננתח אותו.

הסברת הזיהוי בלוג



דבר ראשון, נבדוק את הsourceAddress, במקרה זה, 195.1.144.109, להלן תמונה.

sourceAddress	s
195.1.144.109	r

נלך לאתר <https://www.ipqualityscore.com> בכדי לחפש את הכתובת IP הזו.

ונראה שהיא Blacklisted, ושהיא לא כתובת לגיטימית בעליל.

Check IP Reputation for 195.1.144.109

IP Address	195.1.144.109
Proxy/VPN Detection Check	 Reputation Issues Detected This IP address has been detected as a proxy connection, which could be hurting your IP reputation.
IP Reputation Score	99% - Abusive IP
Blacklist Checks	IP reputation issues detected, we recommend removing your IP address from the following blacklists to improve your reputation score. <div>Blacklisted by Spamhaus Blacklisted by FMB BL</div>
Country	NO 
CIDR IP Address Subnet	195.1.144.0/24



Perform a Full IP Address Lookup on 195.1.144.109

דבר שני, ניתן לראות שהבקשה ניסתה להפעיל פקודה מסוכנת בשם "wget". פקודה זו מאפשרת הורדת קבצים מהאינטרנט.

ולהוריד קובץ משרת בכתובת 103.14.226.142 כעת נכנס לאותו אתר שנכנסנו אליו קודם, ונראה מה הם אומרים עליו.

ניתן לראות 96% שזו כתובת זדונית, אשר נמצאת בוויטנאם.

Check IP Reputation for 103.14.226.142

IP Address	103.14.226.142
Proxy/VPN Detection Check	 Reputation Issues Detected This IP address has been detected as a proxy connection, which could be hurting your IP reputation.
IP Reputation Score	96% - Abusive IP
Blacklist Checks	IP blacklist check passed, this IP address was not detected on popular blacklists
Country	VN 
CIDR IP Address Subnet	103.14.226.0/24

Perform a Full IP Address Lookup on 103.14.226.142

HostNamen שעליו הוא מנסה להריץ אותו הוא web.seesec.co.il, ניתן לראות שהתוקף מנסה לבצע פעולת התקפת Command Injection בשרת. הפעולה מתבצעת דרך כתובת ה-URL המופיעה בלוג.

על Command Injection

התוקף מנסה להוריד קובץ בשם "shk" מכתובת מסוימת ולהריץ אותו עם הרשאות גבוהות על ידי Command Injection. הפעולה נראית כאילו התוקף מנסה לקבל שליטה על השרת או להוריד תוכנה זדונית על מנת לבצע פעולות לא רצויות.

דעתי על האירוע, תקין?, יש צורך בהרחבת החקירה?

דעתי, ואני חושב שהיא לא בהכרח דעה, היא עומדת בקו עובדה, היא דורשת המשך חקירה, בלי ללכת רחוק מדי, רק הכתובות IP, מאיפה שהגיע הבקשות, ומאיפה שלהוריד את הקבצים, כבר מדליק נורה אדומה, אדומה מאוד.

ועצם זה שזה עבר את החומת אש, אומר המון.

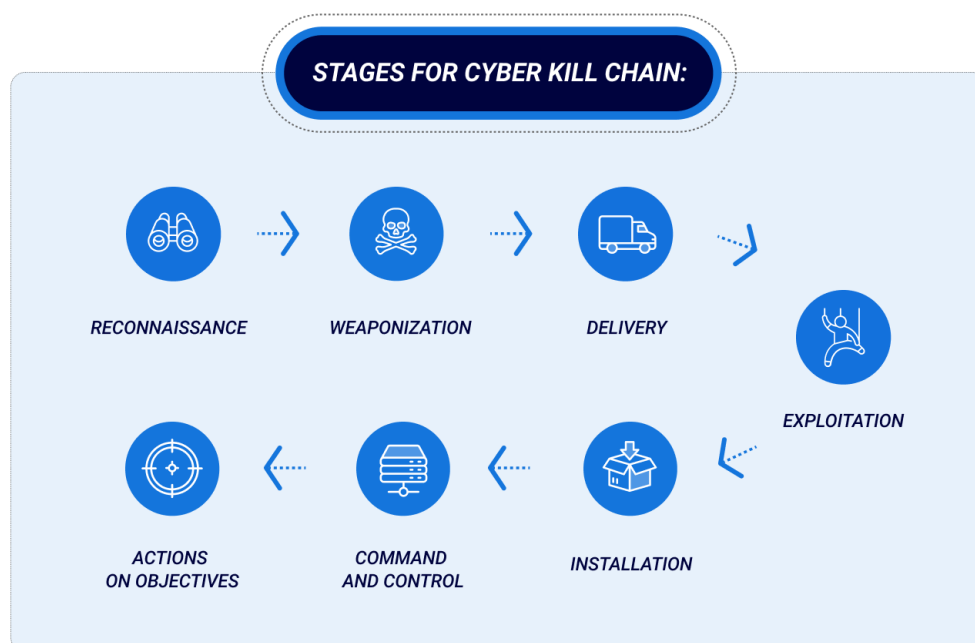
מה החקירה שהייתי מבצע?

דבר ראשון בודק את הקובץ shk, הייתי רוצה לנתח אותו, להבין מה מטרתו, והאיומים שהוא באמת מהווה.

הייתי בודק את המערכת בכללי, מחפש פגיעויות, לבדוק שלא הורד משהו שהחומת אש העבירה, ולא קיבלתי עליו התראה.

באיזה שלב ב Cyber Kill Chain מדובר בעצם?

להלן, Cyber Kill Chain



The Cyber Kill Chain Explained

לפי מה שידוע לנו, ניתן לקבוע כי אירוע האבטחה המתואר נמצא בשלב "ניצול" (Exploitation) ב Cyber Kill Chain.

הבקשה ניסתה להפעיל פקודה בשם "wget". פקודה זו מאפשרת הורדת קבצים מהאינטרנט, וכנראה שהתוקף ניסה להשתמש בה כדי להוריד קובץ לכאורה זדוני מכתובת IP לא אמינה במיוחד.

הבקשה הצליחה לעקוף את חומת האש. זה מעיד על כך שהתוקף הצליח **לנצל** פגיעות במערכת כדי לחדור אליה.

אך חשוב מאוד לציין, שמאוד אפשרי שהאירוע התקדם מעבר לשלב ה"ניצול" בשרשרת התקיפה.

איזה טכניקה או טקטיקה מדובר מתוך MITRE

מדובר בטכניקת (T1059) Command and Scripting Interpreter

התיאור של הטכניקה:

"תוקפים עשויים לנצל מתורגמנים של פקודות ותסריטים כדי להפעיל פקודות, תסריטים או קבצים בינאריים. ממשקים ושפות אלה מספקים דרכים לניהול של מערכות מחשב והם תכונה נפוצה במגוון פלטפורמות שונות. רוב המערכות מגיעות עם ממשק שורת פקודה ויכולות תסריטאות מובנים, לדוגמה, מערכות הפעלה מסוג macOS והפצות לינוקס כוללות גרסה כלשהי של Shell של Unix בעוד שבהתקנות של Windows כלולות Windows Command Shell ו-PowerShell.

קיימים גם מתורגמנים הפועלים על גבי פלטפורמות שונות כמו Python, כמו גם אלו המזהים בדרך כלל עם יישומי לקוח כמו JavaScript ו-Visual Basic. תוקפים עשויים לנצל לרעה טכנולוגיות אלו בדרכים שונות כדי להפעיל פקודות שונות. פקודות ותסריטים יכולים להיות משוכנים בתוכנות גישה ראשונית (Initial Access) המסופקות לקורבנות כמסמכי פיתיון או כתוכנות משניות המורדות מ-C2 קיים (שרשרת פיקוד והשליטה). תוקפים עשויים גם להפעיל פקודות באמצעות מסופים/שורות פקודה אינטראקטיביות, כמו גם לנצל שירותים מרוחקים שונים כדי לבצע ביצוע מרחוק." (תורגם על ידי Gemini, בכדי להיכנס לטכניקה ניתן ללחוץ [כאן](#))

כעת אסביר מדוע אני חושב שזו הטכניקה:

תיאור הלוג מציג ניסיון להפעיל פקודה בשם "wget" - פקודה זו משמשת להורדת קבצים מהאינטרנט, וייתכן שהתוקף ניסה להשתמש בה כדי להוריד קובץ זדוני.

תיאור MITRE תואם לפעולה בלוג: תיאור הטכניקה מציין שתוקפים עשויים לנצל ממשקי Command Line ובאמצעות scripting כדי להפעיל פקודות, סקריפטים או קבצים על מערכות.

אירוע 2

קיבלנו מייל מאבי וויסמן, איזה מגניב.

From name: avi.waisman

From E-mail: 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

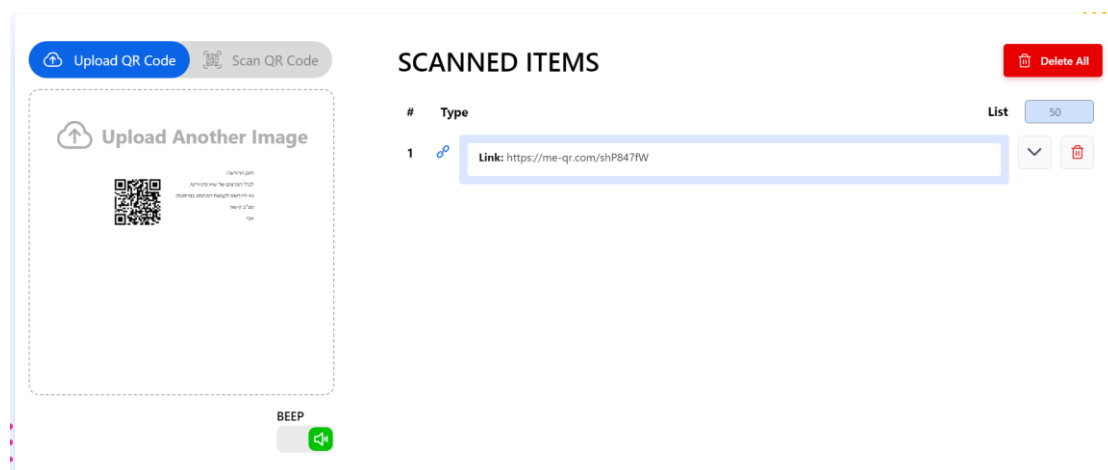
מצ"ב קישור

אבי

לחקור את המייל, האם מדובר במייל פשינג?

דבר ראשון שנסתכל, זו הכתובת שממנה קיבלנו את המייל, מתכוון כמובן לדומיין, שהדומיין הוא אמיתי, מאחר ואני מכירים את הדומיין ניתן לראות שזה באמת מהימן, אך בכל אופן קיימים דרכים לזייף דברים כאלו, נחקור מה זה ה QR הזה, ניתן לאיזה אתר לבדוק מה זה הקישור הזה.

נלך לאתר <https://qrscanner.net>, וניתן לו את הqr הזה, ולהלן התוצאה.



כעת ניתן לראות שהשתמש במקצר כתובת, יעיל לשימוש ללינקים ארוכים, הרבה משתמשים בזה שמעבירים קישורים, במיוחד זדוניים, נכנס לאתר <https://checkshorturl.com> ונראה מה הוא אומר על הקישור שאבי העביר לנו.

וניתן לראות שזה באמת קישור לפייסבוק, וזה לא מייל פשינג.

CheckShortURL

Expand and verify all your shortened links

CheckShortURL supports a wide range of URL shortening services, including t.co, goo.gl, bit.ly, amzn.to, tinyurl.com, ow.ly,youtu.be, and many others.

Expand

You made 1 request out of 120 in the last 24 hours.

Short URL	<div>https://me-qr.com/shP847fW</div>
Long URL	<div>https://www.facebook.com/unsupportedbrowser</div>
Code	<div>302</div>
Screenshot	

סיכום של מה חקרנו ואיך הגעתי למסקנה שלי

דבר ראשון שעשינו הוא בדיקה של הדומיין שממנו קיבלנו את המייל, למרות זאת, אנו יודעים שניתן לזייף כאלה מיילים בקלות כיום, והלכנו ובדקנו מה הקישור שמתקבל בQR, וקיבלנו קישור מקוצר, את הקישור המקוצר שמנו ב"מפרק" קישורים מקוצרים, וראינו שאנחנו מקבלים באמת את פייסבוק, בדומיין האמיתי שלהם. כך הגענו להבנה מלאה, שזה הוא לא פשינג.

במידה ומדובר במייל פשינג איזה פעולות הייתי מבצע

הייתי מספר לחבריי המרצים, שכנראה גם הם קיבלו מייל כזה, שיזהרו, לא הייתי כמובן לוחץ או נכנס לשום קישור, הייתי מדווח אותו כמייל ספאם.

על איזה שלב בCyber Kill Chain מדובר

מייל פשינג יכול להתאים לשלב ה-"Weaponization" ב Cyber Kill Chain

תרגום של התיאור מה זה השלב הזה, מתוך [pcmatic](https://www.pcmatic.com)

"בשלב זה, הפושע יוצר וקטור תקיפה או נתיב חדירה. זה למעשה בחירת הנגיף או השיטה דרכה הוא יקבל גישה למערכת היעד. התוקף עשוי להשתמש בתוכנה זדונית, תוכנת כופר, וירוס או תולעת אחרות, או אפילו במתקפת פשינג כדי לקבל גישה למערכת היעד. בשלב זה, הפושע יכול גם להקים "דלתות אחוריות" כדי להמשיך וליהנות מגישה למערכת אם נקודת הכניסה המקורית נסגרת."

לפי התיאור הזה, מה שקרה פה פשוט מתאים בול לשלב זה, מאחר והיה פה "כביכול" מייל פשינג, כדי לקבל גישה למערכת יעד.

ציינו איזה טכניקה או טקטיקה מדובר מתוך הMITRE

מדובר בטכניקת (T1566) Phishing

תרגום התיאור מMITRE, על הטכניקה.

"פושעים ברשת עשויים לשלוח הודעות פשינג כדי לקבל גישה למערכות הקורבן. כל צורות הפשינג הן הנדסה חברתית המועברת בצורה אלקטרונית. פשינג יכול להיות ממוקד, המכונה דיג חנית (Spear Phishing). בדיג חנית, הפושע יכוון לאדם, חברה או תעשייה ספציפיים. באופן כללי יותר, פושעים עשויים לבצע פשינג לא ממוקד, כגון במסעות ספאם המוניות של תוכנות זדוניות.

פושעים עשויים לשלוח לקורבנות דואר אלקטרוני המכיל קבצים מצורפים או קישורים זדוניים, בדרך כלל כדי להפעיל קוד זדוני במערכות הקורבן. פשינג ניתן לבצע גם באמצעות שירותי צד שלישי, כגון פלטפורמות מדיה חברתית. פשינג עשוי גם לערב טכניקות של הנדסה חברתית, כגון התחזות כמקור אמין, וכן טכניקות התחמקות כגון הסרה או שינוף של דוא"ל או מטה-נתונים/כותרות מחשבונות פרוצים המשמשים לשליחת הודעות (לדוגמה, כללי הסתרת דוא"ל). דרך נוספת להשיג זאת היא על ידי זיוף או התחזות של זהות השולח שיכול בעצם "לעבוד" גם על האדם שמקבל את המייל, וגם מערכות אבטחה אוטומטיות.

קורבנות עשויים גם לקבל הודעות פשינג המורות להם להתקשר למספר טלפון שם הם מופנים לבקר ב-URL זדוני, להוריד תוכנות זדוניות או להתקין כלים לניהול מרחוק נגישים ליריב במחשב שלהם (כלומר, ביצוע משתמש).

תיאור זה מדבר על קבלת מייל מתחזה, ושליחת קישור לצורך שימוש זדוני, בדיוק התיאור שאנחנו מחפשים.

אירוע 3

יש לנו חוק כזה:

Sysmon

| where CommandLine contains "whoami"

הסבר על החוק, ומה הוא מחפש

החוק מחפש בעצם תחת Sysmon (System Monitor) הוא כלי חנימי של Windows המנטר ורושם פעילויות כמו יצירת תהליכים, חיבורי רשת, טעינת מנהלי התקנים וקבצי-DLL ושינויים של חותמות זמן ליצירת קבצים ביומן האירועים של Windows). לקחתי מפה את ההסבר.

אז החוק מחפש שם בעצם אירועים שהפקודה שהופעלה בCommand Line מכילה את "whoami".

פירוט מהלך החקירה, שאלות שעולות ופירוט

ניתן לראות שאת הפקודות הללו מריץ Jim, הוא רוצה לראות לאן הוא מחובר, והוא רוצה לראות לאיזה קבוצות המשתמש אליו הוא מחובר הוא משוייך

Results	Chart	Add bookmark
1 Sysmon		
2 where CommandLine contains "whoami"		

Product	Company	CommandLine	CurrentDirectory	User	LogonGuid	LogonId
Microsoft® Windows® Operati...	Microsoft Corporation	whoami	C:\Users\jim.WIN10B\Documen...	WIN10B\jim	{0c2a0d71-dc13-6639-e9cd-0d...	0xdcdce9
Microsoft® Windows® Operati...	Microsoft Corporation	whoami	C:\Users\jim.WIN10B\Desktop\	WIN10B\jim	{0c2a0d71-dc13-6639-e9cd-0d...	0xdcdce9
Microsoft® Windows® Operati...	Microsoft Corporation	whoami	C:\Users\jim.WIN10B\Desktop\	WIN10B\jim	{0c2a0d71-dc13-6639-e9cd-0d...	0xdcdce9
Microsoft® Windows® Operati...	Microsoft Corporation	whoami	C:\Users\jim.WIN10B\	WIN10B\jim	{0c2a0d71-dc13-6639-e9cd-0d...	0xdcdce9
Microsoft® Windows® Operati...	Microsoft Corporation	whoami /groups	C:\Windows\system32\	WIN10B\jim	{0c2a0d71-caf0-6617-42ec-290...	0x129ec42
Microsoft® Windows® Operati...	Microsoft Corporation	whoami	C:\Windows\system32\	WIN10B\jim	{0c2a0d71-caf0-6617-42ec-290...	0x129ec42

ParentCommandLine
"C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\Jim.WIN10B\Desktop\Gift.xlsx"

עולות לי רק שלוש שאלות, למה הוא בודק את זה, מה עוד הוא הריץ בסמוך לזה, ולמה זה רץ דרך קובץ Excel בשם Gift?

מה דעתי, האם מדובר באירוע אמת או שווא, ואיך הייתי מטפל באירוע

לדעתי, צריך באותו רגע לבודד את המחשב מהרשת, מדובר סביר להניח באדם מבחוץ שהצליח להתחבר למחשב, והוא רוצה לדעת איפה הוא נמצא, אדם שהוא באמת בעל החשבון, אמור לדעת הכל, ולא צריך להשתמש בפקודת whoami מאחר ואין לו אינטרס בשימוש בה. במיוחד שיש קובץ Excel בשם שמתאים לקובץ שהיה בפשינג שמריץ את זה, לאחר הבידוד ארים טלפון לחברה, ואבדוק האם Jim הוא זה שבאמת הריץ את הפקודות הללו, מדובר באירוע **אמת** לכל דבר ועניין, פקודת whoami שרצה מקובץ אקסל בשם Gift מרימה נורה אדומה באופן **מידי**.

באיזה שלב ב-Cyber Kill Chain מדובר

מדובר בשלב 7, Actions on Objective, תרגום של התיאור של השלב:

"בשלב הלפני אחרון, התוקף מתחיל לבצע את כל מטרותיו המיועדות, כגון הרס, גניבת נתונים, הסתננות, הצפנה וסחיטה."

מתאים לנו לסיטואציה, מאחר וסביר להניח ואדם מבחוץ נכנס למחשב והתחבר למשתמש מתוך החברה, והתחיל להריץ כבר פקודות, בכדי להבין איפה הוא נמצא ומה הרשאותיו.

בונוס - באיזה טכניקה או טקטיקה מדובר מתוך ה MITRE

מדובר בטקטיקת Execution (TA0002)

תיאור מMITRE בעברית:

"הביצוע (Execution) מורכב מטכניקות שגורמות להרצת קוד בשליטת התוקף על מערכת מקומית או מרוחקת. טכניקות שמפעילות קוד זדוני משולבות לעיתים קרובות עם טכניקות מכל שאר הטקטיקות כדי להשיג יעדים רחבים יותר, כגון סיור ברשת או גניבת נתונים. לדוגמה, תוקף עשוי להשתמש בכלי גישה מרחוק להפעלת סקריפט PowerShell שמבצע גילוי מערכת מרוחקת."

ניתן לראות שהתוקף שלנו, בעצם התחבר למחשב, וכעת מסייר ברשת, וכנראה כבר התחיל לגנוב נתונים, כמו הקבוצות שקיימות אצלנו ברשת.