משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

בלמ"ס

TLP: לבן

24 אפריל 2017
כ"ח ניסן תשע"ז
סימוכין: ב-ס-120

גלי תקיפה כנגד גופי ממשל, אקדמיה וגורמים עסקיים בישראל

תקציר

בימים האחרונים זוהו מספר גלי תקיפה כנגד משתמשים שונים בגופי ממשל, אקדמיה, מחקר, וחברות שונות במשק הישראלי.

מקור התקיפה בשרת דוא"ל השייך לגוף אקדמי, וכן בשרת נוסף השייך לחברה עסקית.

מתווה התקיפה עושה שימוש בחולשת WORD (CVE-2017-0199).

התרעה לגבי אפשרות תקיפה במתווה זה פורסמה ע"י ה-CERT ב-12/4/17. סימוכין ב-ס-105.

חברת מיקרוסופט הוציאה עדכון אבטחה המונע את פעילות הפוגען הנ"ל. מומלץ להתקינו בהקדם האפשרי.

פרטים

לו"ז

להלן פירוט גלי התקיפה שזוהו עד כה:

Time	From	Subject	To	Attachment	Link
19 Apr 2017 11:54:48 +0300	מוסד אקדמי	::NIH cancer research funding opportunities	נמען יחיד	3.DOC	
19 Apr 2017 14:28:04 +0300	מוסד אקדמי	אישור קבלת מלגה פרטנית - קרן ידע הנדסי אקדמי	54 נמענים	3.DOC	
23 Apr, 2017 6:37:16 AM	מוסד אקדמי	סטודנטים שהתקבלו לתכניות קיץ 2017	נמען יחיד	1.doc	hxxp://82.145.40.46/558.doc
23 Apr, 2017 6:38:51 AM	מוסד אקדמי	Summer programs - students from India	נמען יחיד	1.doc	hxxp://82.145.40.46/558.doc
23 Apr, 2017 6:40:11 AM	מוסד אקדמי	Schedule an appointment- Apply A2 visa	נמען יחיד	1.doc	hxxp://82.145.40.46/558.doc
23 Apr, 2017 6:44:07 AM	מוסד אקדמי	International Programs	נמען יחיד	1.doc	hxxp://82.145.40.46/558.doc
Sun 4/23/2017 9:55 AM	מוסד אקדמי	נוסחאון לבחינה בתורת	82 נמענים	1.doc	hxxp://82.145.40.46/558.doc
23/4/17 11:34 AM	חברה מסחרית	שנה טובה	106 נמענים	2.doc	hxxp://82.145.40.46/558.doc

<u>פרטים על הפוגען</u>

הפוגען מתנהג באופן זהה למתקפה קודמת המוכרת בשם OILRIG. אינדיקטורים לזיהוי הפוגען ופעילות OILRIG באופן כללי ניתן למצוא בנספח א'.

<u>דרכי התגוננות וזיהוי</u>

חברת מיקרוסופט הוציאה עדכון אבטחה המונע את פעילות הפוגען הנ"ל.

מומלץ להתקין העדכון בהקדם האפשרי בכל עמדות המשתמשים בארגון.

נדרש להוריד את הקובץ הרלוונטי לעדכון בלינק הבא. יש לחפש ע"פ 2017-0199 בשדה CVE.

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199

מוצע להיעזר ברשימת האינדיקטורים המופיעה בנספח א' ולהזינה במערכות אבטחה רלוונטיות כגון שרתי FW, מערכות PROXY, מערכות אנטי-וירוס וסינון תוכן וכו'.

במידה שקיים חשד כי עמדה מסוימת כבר נדבקה בפוגען, ולא ניתן לפרמט את העמדה ולהתקינה מחדש, ניתן לנסות ולבצע הסרה ידנית של הפוגען. הנחיות ההסרה מופיעות בנספח ב'.

במידה שבבדיקתכם התגלה ממצא כלשהו, נבקש לקבל היזון חוזר.

לכל מידע נוסף ניתן לפנות אלינו.

הערה: שיתוף מידע עם ה- CERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כל שהוא, במידה שהתגלה צורך כזה.

בברכה,

CERT-IL

טל: 072-3990800

team@cert.gov.il

נספח א'

1. **Files name:**
   - **a.** 3.doc
     - **MD5:** 1318a321b1afb2934ff20a3fb686ce77
     - **MD5:** 293239948c256f168de06299ffd2845b
   - **b.** JuniperSetupClientInstaller.exe
     - **MD5:** 9ded8101ca5d35039cc4d13d903f71db
   - **c.** OxfordSymposiumRegTool.exe
     - **MD5:** a539b9ea0c4bbfab68e8ecd1ec0b5eee
   - **d.** GoogleSyncCore.exe
     - **MD5:** 8ea471b4065b261d4055be7b595bec2c
   - **e.** GoogleUpdateCore.exe
     - **MD5:** 19525a7511756158c896b28e223a44bc
   - **f.** Test5.hta
     - **MD5:** 8a5ec9425bb3826cac948d0639f3145b
     - **MD5** 2cf04755371a24b2efd380076c7252ca

g. 0011.ps1
- **MD5:** 48999fb7f727a9ed78250e10926d9226
- **MD5:** 31321fd937cfd4cd9778e9ea68af60b0

h. Backup1.vbs
- **MD5:** ed53ab4aa0001920aac3f1f41e629e71
- **MD5:** 3caf858f8c20051d679cd0f703bde89a

i. DnE1.ps1
- **MD5:** ce52b2fe9dd9c525bfc311a297a9fb74
- **MD5:** f66fa9735307c29a9968e4250565affc

j. DnS1.ps1
- **MD5:** 312d7a80457cf0e99e3ce87a25242469
- **MD5:** 137fb17495521d96f5d207355c8c7972

k. 1.VBS
- **MD5:** 41c3152aa96d42757ea325817732039a

l. 2.doc
- **MD5:** 871640cd4c4078e8f75bf8767df9011c

m. 1.doc
- **MD5:** 63cfb80afc7749fb02561eb8f5c6c4cd

2. **Schedule task name:**
   a. Google Sync Core
   b. Google Update Core
   c. GoogleUpdateTasksMachineUI

3. **Persistence files and folders:**
   a. %username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SyncInit
   b. %username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\WinInit
   c. %public%\Libraries\RecordedTV
   d. C:\Program Files\Microsoft Idle
   e. C:\Program Files (x86)\Microsoft Idle

4. **IP's:**
   a. 80.82.67.42
   b. 80.82.67.33
   c. 144.217.209.182
   d. 51.255.24.88

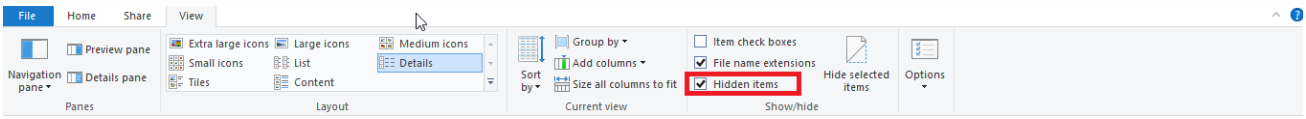
5. **Domains:**
   a. maralen.tk
   b. alenupdate.info
   c. barsupport.org

d. matrix-vpn.com
e. vpsupdate.tk
f. rostuf.info
g. limvpn.com
h. msiupdate.com
i. newusers.tk
j. limvpn.org.in

6. Links
a. http://82.145.40.46/558.doc

נספח ב'

1. ראשית נדרש לאפשר צפייה בפרטים נסתרים (ע"י בחירת הלשונית View וסימון האפשרות Hidden Items - נכון ל-Windows10) -ראה צילום מסך.



2. לגשת לנתיב - C:\Users\Public\Libraries ולוודא כי קיימות בו שתי תיקיות בשם RecordedTV.

במידה שהתיקיות קיימות יש להסיר את התיקייה שאינה בעלת האייקון בצורת הטלוויזיה.
במידה שקיימת רק תיקייה בעלת אייקון בצורת טלוויזיה אין צורך להסירה.

3. לגשת לנתיב - (C:\Program Files\x86) ולוודא כי קיימת בו התיקייה Microsoft Idle.

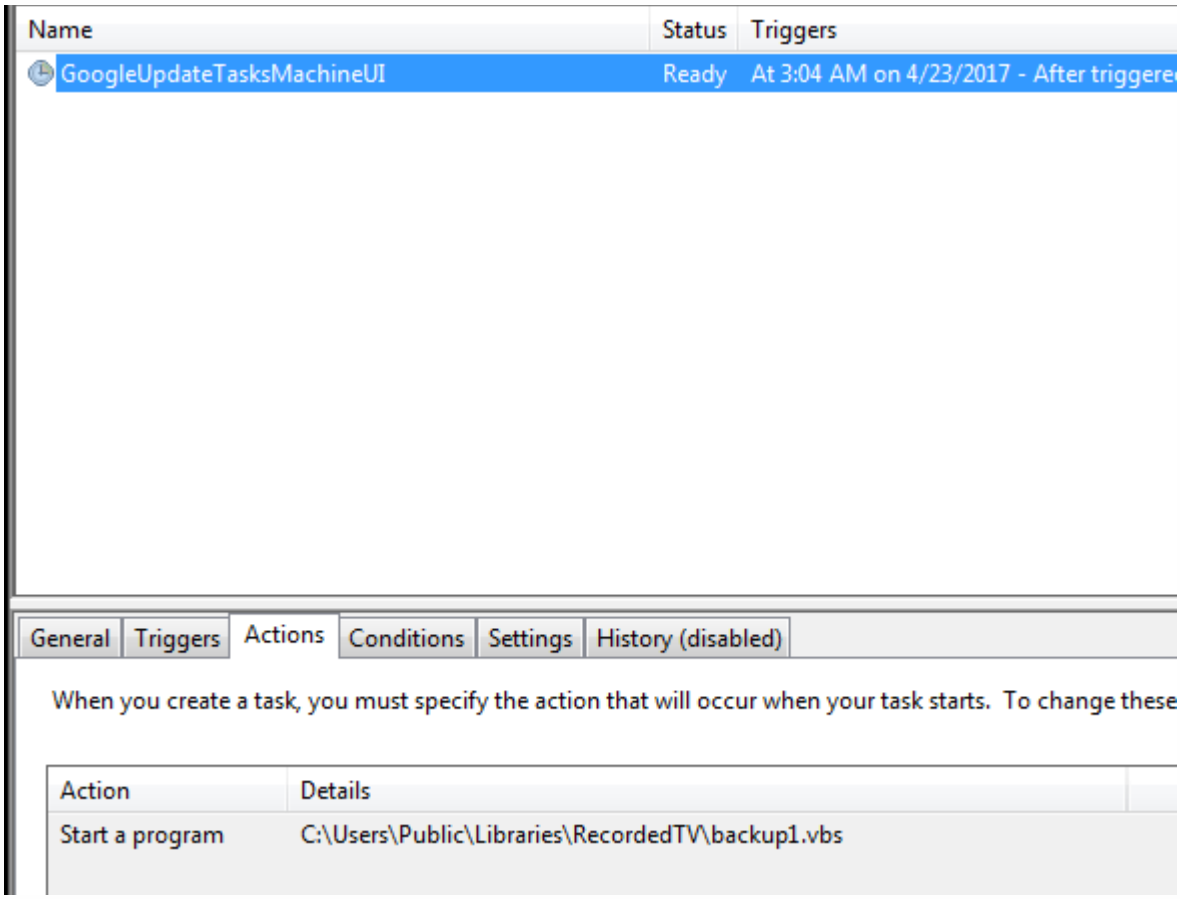
במידה והתיקייה קיימת יש להסירה.

4. לגשת לנתיב %userprofile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup ולבדוק האם נוצרו בו הקבצים SyncInit.lnk, WinInit.lnk.

במידה והקבצים קיימים יש להסירם.

5. לגשת לאשף המשימות המתוזמנות (משימות מתוזמנות או Scheduled Tasks) ולבדוק האם מוגדרת משימה מתוזמנת בשם - GoogleUpdateTaskMachineUI המתחילה מהנתיב בסעיף הנ"ל -ראה צילום מסך.

במידה והמשימה קיימת יש להסירה.



6. לבדוק באשף המשימות המתוזמנות האם קיימת משימה מתוזמנת בשם- Google Sync Core.

במידה והמשימה קיימת יש להסירה.

7. לבדוק האם קיימים ערכי ה-Registry:

REGISTRY\MACHINE\Software\Microsoft\Tracing\powershell_RASAPI32\

REGISTRY\MACHINE\Software\Microsoft\Tracing\powershell_RASMANCS\

במידה שהערכים קיימים יש להסירם.