20 אפריל 2015

א' אייר תשע"ה

סימוכין : י-ס-091

הנדון: התרעה על פוגען הנשלח במתווה של דוא"ל

רקע

לאחרונה התקבל לידי ה- CERT הלאומי מידע אודות פוגען הנשלח במתווה של דוא"ל.

פעילותו של הפוגען זוהתה לראשונה במהלך חודש מרץ 2015, ולעת עתה, עולה כי הוא תקף כבר מספר יעדים בישראל.

תהליך התקיפה

- וקטור התקיפה - מייל המכיל קישור להורדת הפוגען.
- בעת לחיצה על הקישור מורד אוטומטית למחשב הקורבן קובץ מכווץ בשם vlkhdn.gz.
- הקובץ המכווץ מכיל קובץ exe שמופעל ידנית בעת לחיצה כפולה.
- הפוגען מבצע את הפעולות הבאות :
  1. יוצר קובץ pdf בתיקיית %temp% ומפעיל אותו.
  2. מעתיק עצמו לתיקיית %temp%
  3. מעתיק עצמו לתיקיית stratup לצורך שרידות.
  4. מעביר את השירות BITS שאחראי על עדכוני windows למצב הפעלה ידנית.
  5. יוצר תקשורת מול שרתי פיקוד ושליטה בפרוטוקול http לצורך הורדת פוגענים נוספים.

יכולות נוספות של הפוגען

- לצורך הסתרתו, הפוגען רץ כתהליך בשם FoxitReader.exe ברשימת התהליכים במחשב.

מזהים (IOC)

(Indicators Of Compromise) - מאפיינים שנצפו ברשת או במערכת ההפעלה שעשויים להעיד על חדירה או פגיעה במערכות מחשב.

להלן החתימות הידועות ושרתי הפיקוד והשליטה שנצפו בתקיפות נוספות :

(יתכן וחתימות מסוימות לא יופיעו כלל עקב אי הפעלת שלב מסוים, או עקב שינוי בשמות הקבצים, יתכן אף כי גם כתובות ה- IP של שרתי הפיקוד והשליטה משתנות ואינן הכתובות שנצפו בתקיפות שהתגלו)

נתיבי רשת (URL)

- downloadlog.linkpc.net/dw/gtk
- webfile.myq-see.com/dw/gtk
- downloadskype.cf/dw/gtk

תיקיות וקבצים

- %Temp%\FoxReader.exe
- %Temp%\Ambassador.pdf
- Israel's Ambassador to the United States.exe
- vlkhdn.gz

קבצי DLL

- USER32.dll
- ADVAPI32.dll
- NTDLL.dll
- winmm.dll
- WSOCK32.dll
- VERSION.dll
- WINMM.dll
- COMCTL32.dll
- MPR.dll
- WININET.dll
- SleepEx

קבצי רישום מערכת (Registry)

- HKLM\SYSTEM\ControlSet001\services\BITS
- HKLM\SOFTWARE\MozillaPlugins\@adobe.com/FlashPlayer
- C:\Windows\System32\Macromed\Flash\npswf32_11_4_402_278.dll

מחרוזות

- john_1961@gmail.com

Functions

- GetLocalTime
- Sleep
- GetSystemDirectoryA
- FindWindowA
- Process32First
- GetSystemDirectoryW
- SetTimer
- GetVolumeNameForVolumeMountPointW
- GetTokenInformation
- VerifyVersionInfoA

Mutex

- DBWinMutex
- |*|123xXx(Mutex)xXx321|*|6-21-2014-03:06PM

מזהי MD5

- HKf27f25cc3d09944a561feae224f17615
- 079f86600d5bce5f470718301668e285
- adf1bb23d6eb47a0688d0f510b061cad
- 4dfc0e09aec841059024beb823a8c9dd

מזהי SHA-256

- ecde024c622a2b74c0bc69431c3c2cd0a4ba6e3346b6049a62149050eb0c3415
- e8f04d965be7533eedd4115a3b857ae80268eecb11a75d7e3a108e301da7d8e1
- 7c578dcdcefe78fb1dd51ac611f6450d9eb5be6c5f1e3363f460321a46be4a39
- d83ee08469cf58be4ec9ad6d083e46cd3543d4002b82e33ce68fc96e3e2e76e5

מזהי SHA-1

- b5e5cb4bdc571b4b00315a3a119f2d0417c96ec0
- 961dc6c53ff1dd74876160cdc1ed96dd35dd0c73
- 0be09d4feaa50f3946d20caabda070981e9d9472
- e0efd872286480ab782d92baa0841d5db30f7f0d

מזהי SHA- 512

- 0e1470ada2039f169182b9c199379292401732c8863c40aa55bc25665fff9f444aeb61164b6e8da76e08c34b1b45da0594f836815fbc731b95ba4e9e83080838
- 2e1ca60e7997f325b0ea1329b6e041aafb167594a5a7c0fe4075bbefc92f7d71713bc248d2d20f49ef6a73bb547806896401152cca0c4c40fc60a79fb228d961
- 4240cd796fe4f338263baa574be4f6ec720602f8fc1379f002263a0c57cb7148dd140982a4ee1b47752e4c910f7d678fff6b8cada2d1ad7f45879a18bc3c5851
- 04ce78f7a04f1179c63e12afc8ea5660fc865abd81fde26a7a59542b3f75def968eb350b0546499474da0d63332d13feec54dd77b4a8a7169ec9bac708a5485c

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 והתגלה צורך כזה.

בברכה,

CERT-IL

טל: 03-7450801

team@cert.gov.il