16 יוני 2015

כ״ט סיון תשע״ה

סימוכין : י-ס-127

הנדון: התרעה על פוגען Grabit Hawk Eye

תיאור: הפוגען "Grabit Hawk Eye" הינו פוגען המתפשט באמצעות דבוקה המצורפת לדוא״לים.

הדבוקים הינה קובץ word המכיל פקודת מאקרו. הפעלת פקודת המאקרו גורמת להדבקת המחשב בנוזקה בעלת יכולת גניבת מידע באמצעות הסנפת הקשות מקלדת, צילומי מסך וכדומה.

על פי דו״ח של חברת אבטחת המידע קספרסקי, מפת היעדים של הפוגען כוללת מדינות רבות, בהן ישראל.

מזהים (IOC)

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

להלן החתימות הידועות ושרתי ה-C&C 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 ה- C&C משתנות ואינן הכתובות שנצפו בתקיפות שהתגלו)

כתובות IP :

- 31.220.16.147
- 204.152.219.78
- 128.90.15.98
- 31.170.163.242
- 185.77.128.65
- 193.0.200.136
- 208.91.199.223
- 31.170.164.81
- 185.28.21.35
- 185.28.21.32
- 112.209.76.184

תיקיות וקבצים (Files):

- C:\Users\%username%\AppData\Roaming\Microsoft\AudioEndpointBuilder.exe
- C:\Users\%username%\AppData\Roaming\Microsoft\BrokerInfrastructure.exe
- C:\Users\%username%\AppData\Roaming\Microsoft\WindowsUpdate.exe
- %temp%\Gr347.exe

URLs:

- weddings.bz/newz.php

מזהי MD5 שנמצאו:

- bfc30332b7b91572bfe712b656ea8a0c

מזהי SHA-256 שנמצאו:

- bc97038788f52ad6f37275334e8fbe2ab832d7f59777efaed6deaeeb691886e9
- 9b48a2e82d8a82c1717f135fa750ba774403e972b6edb2a522f9870bed57e72a
- ea57da38870f0460f526b8504b5f4f1af3ee490ba8acfde4ad781a4e206a3d27
- 0b96811e4f4cfaa57fe47ebc369fdac7dfb4a900a2af8a07a7b3f513eb3e0dfa
- 1948f57cad96d37df95da2ee0057dd91dd4a9a67153efc278aa0736113f969e5
- 1d15003732430c004997f0df7cac7749ae10f992bea217a8da84e1c957143b1c
- 2049352f94a75978761a5367b01d486283aab1b7b94df7b08cf856f92352166b
- 26c6167dfcb7cda40621a952eac03b87a2f0dff1769ab9d09dafd09edc1a4c29
- 2e4507ff9e490f9137b73229cb0cd7b04b4dd88637890059eb1b90a757e99bcf
- 3928ea510a114ad0411a3528cd894f6b65f59e3d52532d3e0c35157b1de27651
- 710960677066beba4db33a62e59d069676ffce4a01e63dc968ad7446158f55d6
- 7371983a64ef9389bf3bfa8d2abacd3a909d13c3ee8b53cccf437026d5925df5
- 76ba61e510a340f8751e46449a7d857a2d242bd4724d0d040b060137ab5fb31a
- 78970883afe52e4ee846f4a7cf75b569f6e5a8e7a830d69358a8b33d186d6fec
- 7c8c3247ffeb269dbf840c7648e9bfaa8cf3d375a03066b57773c48de2b6d477
- 7f0c4d3644fdcd8ac5bc2e007bb5c3e9eab56a3d2d470bb796af88125cd74ac9

מזהי SHA-1 שנמצאו:

- 3f77403a64a2dde60c4962a6752de601d56a621a
- 4E7765F3BF73AEC6E350F412B623C23D37964DFC

מחרוזות:

- HawkEye_Keylogger_Execution_Confirmed_<VICTIM> 3.10.2015 6:08:31 PM

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

cert.gov.il