10 פברואר 2016

א' אדר א תשע"ו

סימוכין: ל-ס-167

הנדון: התרעה על פוגעני TeslaCrypt

רקע:

בשבועות האחרונים מזוהה גל תקיפה נרחב נגד אתרים ויעדים ישראליים באמצעות פוגען כופר (Ransomware) מסוג TeslaCrypt.

מטרת מסמך זה לפרט בקצרה את תהליך ואופן פעולת הפוגען וכן דרכי התמודדות. כמו כן, המסמך כולל מזהים אפשריים מוכרים.

דרכי הדבקה

1. גלישה: הדבקה באמצעות גלישה לאתרים המכילים את הפוגענים ו/או מבצעים ניתוב מחדש לאתרים זדוניים אשר מדביקים את המחשבים ע"י הורדת הפוגען למחשב.
2. פתיחת קבצים: הדבקה באמצעות שליחת דוא"ל עם צרופה נגועה (כגון קבצי Word ו-Pdf) וניצול חולשות מוכרות בצרופות.

להלן שני מערכים העושים שימוש באוסף של כלי תקיפה אשר מנצלים חולשות להתקנת הנוזקה:

1. Angler Exploit Kit- משפחת פוגענים המוכרת מזה כשנתיים ומנצלת חולשות של Java, Acrobat Reader, Flash ו-Silverlight. רוב השרתים המארחים את הפוגענים אותרו באוקראינה.
2. Nuclear Exploit Kit – משפחת פוגענים המנצלת חולשות של Java, Acrobat Reader, Flash ו-Silverlight.

שלבי התקיפה

1. הדבקת המחשב והתקנת הפוגען באמצעות יצירת קובץ מסוג EXE. בתיקיית %AppData%.
2. הורדת מפתח ההצפנה מהאינטרנט
3. חיפוש קבצי נתונים והצפנה עם מפתח AES-256 ביט
4. מתן סיומת חדשה לקבצים המוצפנים (משתנה בין הגרסאות). להלן מספר סיומות מוכרות: **.ecc, **.abc, **.micro.
5. יצירת קובץ הנחיות לנתקף בפורמט txt ,html לשחזור הקבצים המוצפנים. קובץ ההנחיות מכיל קישור לאתר ייעודי בו, לכאורה, ניתן לפענח את ההצפנה. כמו כן, באתר זה יופיע גם סכום הכופר הנדרש.

<u>דרכי מניעה</u>

1. עדכון שוטף של טלאי אבטחה למערכות ההפעלה ולתוכנות המותקנות במחשב, בדגש על טלאי האבטחה המופיעים מטה.
2. עדכון חתימות Antivirus וחתימות IDS ייעודיות לגרסת הפוגען הנוכחי באמצעות פניה יזומה לספק האנטי וירוס לבקשת קבלת חתימות מעודכנות.
3. סינון תוכן הגלישה באמצעות Proxy ומימוש URL Filtering מחמיר.
4. סינון תעבורת דוא"ל ארגוני באמצעות Mail Filtering / Mail Relay.
5. הגברת תדירות ביצוע עדכונים וגיבויים למידע הארגוני ושמירה של מספר גרסאות גיבויים לאחור.

<u>דרכי תגובה והכלה מיידיות</u>

כאשר מזהים תחנה החשודה כנגועה בפוגען כופר יש לפעול ע"פ ההנחיות הבאות :

1. ניתוק פיזי / התקשורת של המחשב מהרשת הארגונית.
2. שמירת "תמונת זכרון" (memory dump) באמצעות תוכנה ייעודית ושמירה על Disk on Key ייעודי בגודל של 16gb לפחות.

   (http://www.toolwar.com/2014/01/dumpit-memory-dump-tools.html - DumpIt)
3. כיבוי אלים של המחשב **רק** לאחר שמירת תמונת הזיכרון.

<u>אינדיקטורים (IOC)</u>

(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)

CVE -Angler Exploit Kit:

Product	CVE
IE	CVE-2015-2419 CVE-2014-0322 CVE-2014-1776 CVE-2014-4130 CVE-2013-2551 CVE-2013-7331
Flash	CVE-2015-5560 CVE-2015-5122 CVE-2015-5119 CVE-2015-3113 CVE-2015-3104 CVE-2015-3090 CVE-2015-2419 CVE-2015-0359 CVE-2015-0336 CVE-2015-0313 CVE-2015-0311 CVE-2015-0310 CVE-2014-8440 CVE-2014-8439 CVE-2014-0515 CVE-2014-0497 CVE-2013-5329
Silverlight	CVE-2015-1617 CVE-2013-0074 CVE-2013-3896

Domains:

1. poinformowano.websitesfortrainers.com
2. etailate-rebells.websitesfortrainers.com
3. gmackenziekorntunna.websitesfortrainers.com
4. nopeutunutta-Zeitschriftenverlag.websitesfortrainers.com

5. entelrgy.net
6. websites4all.net
7. ISV.isigmasystems.net
8. isigmasystems.net
9. swindlerskateboard.net
10. john grant.codes
11. tapdanceshoes.us
12. thesnoringowl.com
13. fiveleafvinyard.com
14. applegateweedworkers.com
15. getoor-riccibit.applegateweedworkers.com
16. assassinaviravate.applegateweedworkers.com
17. earthwar-mail data.applegateweedworkers.com
18. zeitsparendem-accidere.applegateweedworkers.com
19. embezzlementeconomicpolicy.applegateweedworkers.com
20. minnetonkauniversity.com
21. rhythmtapshoes.net
22. kontrollogikidiotyzm.rhythmtapshoes.net
23. destituaveram.Dothy.com

IP:

1. 185.46.8.218
2. 195.64.155.168

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: 03-7450801

team@cert.gov.il