



העדכון שלפניכם לוקט ועובד במסגרת פעילות ה-CERT הלאומי על בסיס מגוון מקורות רחב, כדי לרכז מידע רלוונטי ואקטואלי לעוסקים בתחום הגנת הסייבר. כפועל יוצא, ה-CERT הלאומי אינו יכול לערוך לחלוטין למידע המובא בעדכון או למסקנות המשתמעות ממנו, ואין באמור בעדכון משום המלצה לנקיטת פעולות כלשהן או לשינוי מדיניות אבטחה קיימת. אין באזכור חברות אבטחה או גורמים מסחריים אחרים משום הבעת עמדה או המלצה ביחס אליהם או לשירותים או המוצרים המוצעים על ידם.

19 אפריל 2015

ל' ניסן תשע"ה

סימוכין: י-ס-093

## הנדון: התרעה על פוגען CryptoWall 3.0 Ransomware

### רקע:

מידע שהתקבל לאחרונה ב-CERT הלאומי מצביע על גלי תקיפה באמצעות דוא"ל המכיל צרופה נגועה בפוגען כופר (Ransomware) מסוג CryptoLocker.

### שלבי תקיפה:

1. הפוגען מופץ באמצעות דוא"ל ספאם, שעל פי רוב נשלח באמתלה של קורות חיים, אולם לא מצורפים אליו קבצי PDF, DOC או RTF. לדוא"ל מצורפים קבצי JS (JavaScript), אשר נמצאים בתוך קובץ zip. קבצי ה-JS (JS\_DLOAD.CRYP, JS\_DLOADR.JBNZ ו-JS\_DLOADE.XXPU) מחולצים מתוך קובץ ה-zip.
2. קבצי ה-JS מתקשרים עם שתי כתובות URL על מנת להוריד קבצי JPG, לכאורה. אולם הסיומת הזו נועדה לעקוף מערכות זיהוי חדירה (IDS) בלבד, וקבצים אלו הם למעשה קבצי EXE.
3. קובץ התמונה הראשון (one.jpg), אשר מזוהה כ-TROJ\_CRYPWAL.YOI, יוצר instance חדש של explorer.exe בכדי לקבל הרשאות אדמיניסטרטור, זאת בהינתן שלקורבן יש כבר הרשאות אדמיניסטרטור. שימוש ב-process לגיטימי כמו explorer יכול לעזור לפוגען לעקוף סורקים המשתמשים ב-Whitelisting.
4. הקובץ יוצר instance חדש של svchost.exe אשר יבצע תקשורת מול שרת ה-C&C והצפנת קבצים.
5. הקובץ מוחק עותקי-צל (Shadow Copies), על מנת למנוע אחזור של המידע לאחר הצפנתו ע"י הנתקף.
6. לאחר קבלת מפתח הצפנה פומבי מסוג RSA משרת ה-C&C, ולאחר שמירת המפתח הפרטי אשר נועד לפענוח ההצפנה על השרת, מתחילה הצפנת קבצים מסוגים שונים: מסמכים, בסיסי מידע, דוא"ל, תמונות, קבצי שמע, קבצי וידאו וקודי-מקור.
7. לאחר ההצפנה באלגוריתם RSA-2048, תתווסף לקובץ המוצפן סיומת אקראית, ולתיקיות המוצפנות תתווסף הסיומת "HELP\_DECRYPT". לאחר מכן תוקפץ בפני הקורבן הודעת הסחיטה המבקשת תשלום בתמורה לפענוח הקבצים המוצפנים.
8. בעוד שדעתו של הקורבן מוסחת ע"י הודעת הסחיטה, קובץ התמונה השני (two.jpg), אשר מזוהה כ-TSPY\_FAREIT.YOI, מריץ רוגלה על המחשב. הרוגלה גונבת Credentials מ-FTP Clients, דפדפנים, Email Clients ומארנקי Bitcoin.

ניתן לשתף מידע המסווג "ירוק" עם כל הגורמים העשויים לעשות בו שימוש מועיל. עם זאת, אין לשתף בערוצים פומביים, דוגמת אתרי אינטרנט, רשתות חברתיות ואמצעי תקשורת המונים.



9. זוהי הפעם הראשונה שפוגען הכופר נשלח יחד עם רוג'לה. קפיצת מדרגה זו מאפשרת לתוקפים לגנוב כסף מהנתקפים גם אם האחרונים ממאנים להיענות לדרישתם.

### אינדיקטורים (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)

### :Domains

- sehpan.com
- bn369.com
- drdigitalmd.com
- youngprofreshional.com
- bijouxbjx.com
- sam73cyber.com
- ineshworld.com
- sooimchae.com
- ouarazateonline.com
- bikeviet.com
- futong8.com
- ocvitcamap.com
- filemade.com

### :IP

- 188.124.7.10
- 182.50.142.7
- 23.250.14.111
- 173.254.28.120
- 37.221.161.69
- 66.23.237.186
- 199.204.44.246
- 112.175.184.31
- 216.55.179.136
- 108.166.217.2
- 112.78.7.162



### תיקיות וקבצים (Files):

- two.jpg
- 33866092.bat
- one.jpg
- %appdata%\3efba0e4.exe \*
- C:\Documents and Settings\%username%\Start Menu\Programs\Startup\3efba0e4.exe\*
- RegularSquatting.exe
- RuleReputable.exe
- C:\3efba0e4\3efba0e4.exe \*

\* - התווים שלפני ה-exe יכולים להופיע כשמונה תווים שונים

### קבצי רישום מערכת (Registry):

- HKU\S-1-5-21-1409082233-688789844-725345543-1003\Software\Microsoft\Windows\CurrentVersion\Run
- HKU\S-1-5-21-1409082233-688789844-725345543-1003\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKU\S-1-5-21-1409082233-688789844-725345543-1003\Software\Microsoft\Windows\CurrentVersion\Run
- HKU\S-1-5-21-1409082233-688789844-725345543-1003\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\SYSTEM\ControlSet001\Services\wscsvc
- HKLM\SYSTEM\ControlSet001\Services\BITS
- HKLM\SYSTEM\ControlSet001\Services\ERSvc
- HKLM\SYSTEM\ControlSet001\Services\wuauerv
- C:\3efba0e4\3efba0e4.exe \*
- C:\3efba0e4\3efba0e4.exe \*
- C:\Users\%username%\AppData\Roaming\3efba0e4.exe \*
- C:\Users\%username%\AppData\Roaming\3efba0e4.exe \*

\* - התווים שלפני ה-exe יכולים להופיע כשמונה תווים שונים



**:Deleted registry**

- HKU\S-1-5-21-1409082233-688789844-725345543-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings
- HKU\S-1-5-21-1409082233-688789844-725345543-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings
- ProxyOverride
- AutoConfigURL

**:String**

- 986aun46iys608
- hlqqo7fv0rz7dm
- tjd15zays8g25
- 30ozw8t3liqu

**מזהי MD5 שנמצאו:**

- 58a9208f31a646881b8776b5834aad4d
- 4eec9d50360cd815211e3c4e6bdd08271b6ec8e6
- 7e7490a49ccc138dd7ac701354cd88f7
- 3880eeb1c736d853eb13b44898b718ab
- 10a3a678c0f3f2b81d152f67ab1626b2

**מזהי SHA-256 שנמצאו:**

- cbbeebe03ebd38a1213dd6b0773524f8a878e59e92cbd2578bcd6089bdeda902
- 662122dacfa61d8f2580fc97dfd8b0c89d319bdbab2b0275c4dcf638e71301c2
- 936d9411d5226b7c5a150ecaf422987590a8870c8e095e1caa072273041a86e7
- 87b9e342bdb6ce7e87ff9022979858879794434f521603408eb2bf595f58634c

**מזהי SHA-1 שנמצאו:**

- 0e70b9ff379a4b2ea902d9ef68fac9081ad265e8
- 936d9411d5226b7c5a150ecaf422987590a8870c8e095e1caa072273041a86e7
- a3a49a354af114f54e69c07b88a2880237b134fb
- 47363b94cee907e2b8926c1be61150c7



- ca963033b9a285b8cd0044df38146a932c838071
- c39125e297f133ddfe75230f9d2c7dc07cc170b3
- 6094049baeac8687eed01fc8e8e8e89af8c4f24a
- 0C615B3DB645215DEC2D9B8A3C964341F777BC78
- 7481061f71d204f5cdb18c80b32c7eaf8b749d4d

**מזהי SHA-512 שנמצאו:**

- cd9227f4e6633bc79c7481463b6ab5b3c2235b9ec8cf170b26440e79b9c435e0d054f949fb066205b4cbe846c6d8126b7b05cc813ca2cb42cd655df4611524a9
- 8d493832992ce1952b9caec4223c3587f2f0d441324bec7b0d0fa907d3d654a523146c51a30c6cbcd67124916f82fdd99e988031b709af2c7482a6c755db328a
- 93dfaafc183360829448887a112dd49c90ec5fe50dcd7c7bbc06c1c8daa206eeea5577f726d906446322c731d0520e93700d5ff9cefd730fba347c72b7325068
- 589506a1da7ea399447f9308d0c9a028efd4301d3b97abe7a35fc227e9053b2cda6c9e206365239fc3e55070742fbb7611f28894d9f4e319f080f95d4adce2a4

**:Path**

- drdigitalmd.com/img1.php?w=30ozw8t3liquc
- youngprofreshional.com/img1.php?v=30ozw8t3liquc
- sooimchae.com/img4.php?o=986aun46iys608
- ouarazateonline.com/img3.php?t=986aun46iys608
- bikeviet.com/img1.php?s=986aun46iys608
- futong8.com/img5.php?j=986aun46iys608
- ocvitcamap.com/administrator/lib/cheapoakley.php
- filemade.com/img2.php?i=986aun46iys608
- ineshworld.com/img3.php?q=986aun46iys608
- drdigitalmd.com/img1.php?l=tjd15zays8g25
- youngprofreshional.com/img1.php?t=tjd15zays8g25
- drdigitalmd.com/img1.php?a=hlqqqo7fv0rz7dm
- youngprofreshional.com/img1.php?l=hlqqqo7fv0rz7dm

**:DLLs**

- user32.dll
- gdi32.dll



### :Mutexes

- Global\CLR\_CASOFF\_MUTEX
- CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-1004MUTEX.DefaultS-1-5-21-1547161642-507921405-839522115-1004
- \_!MSFTHISTORY!\_
- c:\documents and settings!user!local settings!temporary internet files!content.ie5!
- c:\documents and settings!user!cookies!
- c:\documents and settings!user!local settings!history!history.ie5!
- WininetStartupMutex
- WininetConnectionMutex
- WininetProxyRegistryMutex
- ShimCacheMutex
- Groove:PathMutex:[LUt+jL/YbxUWwjk7hRky++rqRco=]
- Global\CLR\_CASOFF\_MUTEX
- CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-1004MUTEX.DefaultS-1-5-21-1547161642-507921405-839522115-1004
- ZonesCounterMutex
- ZoneAttributeCacheCounterMutex
- ZonesCacheCounterMutex
- ZonesLockedCacheCounterMutex

### :Folders

- C:\3efba0e4\*

\* - התווים שלפני ה-*exe* יכולים להופיע כשמונה תווים שונים

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](mailto:team@cert.gov.il)

ניתן לשתף מידע המסווג "ירוק" עם כל הגורמים העשויים לעשות בו שימוש מועיל. עם זאת, אין לשתפו בערוצים פומביים, דוגמת אתרי אינטרנט, רשתות חברתיות ואמצעי תקשורת המונים.