



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.

13 יולי 2015

כ"ו תמוז תשע"ה

סימוכין : י-ס- 137

## הנדון: עדכון מזהים לפוגען CryptoWall 3.0 Ransomware

### רקע:

מידע שהתקבל לאחרונה ב-CERT הלאומי מצביע על גל תקיפה נוסף באמצעות דוא"ל המכיל צרופה נגועה בפוגען כופר Ransomware. התרעה זו מכילה מזהים נוספים בהמשך להתרעתנו שבסימוכין י-ס-093.

### מזהים (IOC)

(Indicators Of Compromise) - מאפיינים שנצפו ברשת או במערכת ההפעלה שעשויים להעיד על חזירה 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 :

- 199.16.199.2-38

### Domains :

- adventuresandtrips.com
- blog.pamieciprzyszlosc.pl
- freetrial.traponline.com
- pulse.8z.com
- gamerexp.com
- jubail4.com
- pictalo.com
- mariewilliams.com.au

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.



- masterpotolkov12.ru
- miamirestorationpros.com
- wlsharedservices.org.uk
- theuniform.com.sg
- naturohealthinternational.com
- www.krwarranty.com

### תיקיות וקבצים (Files):

- C:\[8 random chars]\
- %Temp%\2349358.exe
- C:\[8 random chars]\[8 random chars].exe
- C:\Documents and Settings\%username%\Start Menu\Programs\Startup\2349358.exe
- %temp%\1634869.exe
- C:\Documents and Settings\%username%\Start Menu\Programs\Startup\1634869.exe

### מזהי MD5 שנמצאו:

- 16347f2a4b9bc3abbcdeaf2560847f3e
- 54ebce9d8a81f9613fd020848e8c4297

### מזהי SHA-1 שנמצאו:

- a27091118b41769e1addb32113684fb2e3d55565
- a5d73a5f9fbe284f53ecc925ad12dddf34aa3b0e

### מזהי SHA-256 שנמצאו:

- 6981ee4c4c280b63dacabb95f7033732543a6668e4c3e6e4d0d3da75f0b81e176a  
c85f81d3198d877127c46e92e1c20c68b233672e0eeeb8d7ac8dc78f09b2dd
- 8e92295b77b111b08513c4ff683ae9365cec5b8de7e2adaf0035945d1b44e94a5f  
734091b6e5b6f4f21b7a1c2bffb3363b8cd7aaa8b19fd49f62eb2f72cbcf49



**:URL**

- [campoflor.com/wp-includes/pomo/Circolari.php](http://campoflor.com/wp-includes/pomo/Circolari.php)
- [arabicgermany.com/arabicgermany.com](http://arabicgermany.com/arabicgermany.com)
- [artemis.isolutiontank.com/wp-includes/pomo/i.php](http://artemis.isolutiontank.com/wp-includes/pomo/i.php)
- [beatcancerinms.com//yahoo\\_site\\_admin/credentialspierwsza-pomoc.php](http://beatcancerinms.com//yahoo_site_admin/credentialspierwsza-pomoc.php)
- [canyonsdelmaresme.cat/wp-content/languages/languages.php](http://canyonsdelmaresme.cat/wp-content/languages/languages.php)
- [castleconifer.com/wp-admin/includes/payment.php](http://castleconifer.com/wp-admin/includes/payment.php)
- [cekharga.ariefew.com/wp-includes/certificates/boredbreak.php](http://cekharga.ariefew.com/wp-includes/certificates/boredbreak.php)
- [cekharga.ariefew.com/wp-admin/js/arealsoft2.0.php](http://cekharga.ariefew.com/wp-admin/js/arealsoft2.0.php)
- [christcommunitycogic.org/pwksfmaw/klsjedvbss/th-TH.php](http://christcommunitycogic.org/pwksfmaw/klsjedvbss/th-TH.php)
- [cinema175.com/ecupidthemovie/contact/contact.php](http://cinema175.com/ecupidthemovie/contact/contact.php)
- [www.retetethermomix.ro/wp-includes/fonts/fonts.php](http://www.retetethermomix.ro/wp-includes/fonts/fonts.php)
- [www.savingmummy.com.au/wp-content/upgrade/upgrade.php](http://www.savingmummy.com.au/wp-content/upgrade/upgrade.php)
- [www.schenkdirgesundheit.com/wp-content/plugins/plugins.php](http://www.schenkdirgesundheit.com/wp-content/plugins/plugins.php)
- [www.sumterswebdesign.com/wp-content/themes/throttle.php](http://www.sumterswebdesign.com/wp-content/themes/throttle.php)
- [youngswanky.com/wp-includes/pomo/com\\_jumi.php](http://youngswanky.com/wp-includes/pomo/com_jumi.php)

במידה שבבדיקתכם התגלה ממצא כלשהו נבקש לקבל היוזן 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.