



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 לערוב 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.

21 מאי 2015

ג' סיון תשע"ה

סימוכין : ל-ס-111

הנדון: קבוצת ההאקרים "APT-28" מתכננת מתקפת סייבר נגד בנקים

מידע שהתקבל ב-CERT הלאומי מצביע על חשש שקבוצת ההאקרים "APT-28", המוכרת מתקיפות סייבר נגד יעדים צבאיים, ממשלתיים ותקשורתיים, מתכננת מתקפה נגד יעדים פיננסיים בעולם. הקבוצה ידועה גם בשם "Pawn Storm" ופעילה משנת 2007.

וקטור תקיפה:

הקבוצה משתמשת בנוזקה מפיתוח עצמי, המכונה "Sendit" או "Sofacy", המתפשטת באמצעות דיג מתקדם (Spear-phishing) או במהלך הורדת קבצים מאתרים בעלי פרצות אבטחה. הדיג מתבצע, בין היתר, על ידי שליחת הדוא"ל מכתובת דמה הזזה כמעט לחלוטין לכתובת הקיימת ברשימת התפוצה של הנתקף.

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:

- 176.31.112.10

המידע המובא לעיל לוקט ועובד על ידי CERT-IL במטרה לספק ידע רלוונטי ואקטואלי לעוסקים בתחום ההגנה בסייבר לטובת השכלה וידע כללי. אין במידע זה 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.



שמות מתחם (Domains):

- b-of-americ.com
- osce-military.org
- bbcnewsweek.com
- gov.hu.com
- settings-yahoo.com
- yovtube.co
- googlesetting.com
- cbiuaebn.com
- cbiuaebank.com
- techcruncln.com
- un-unicef.org
- royalbsuk.com
- kwqx.us
- middle-eastreview.org
- unitednat.org
- fbonlinelottery.com
- fubnt.com
- globeshippers.biz
- globeshippers.net
- gsandsc.com
- gshippers.com
- hesselawchambers.com
- largefarm.net
- regionsbnk.info
- regionsbnk.info
- seatreasures.org
- ssandsc.com
- t-d-canadatrust.com
- techielawfirms.com
- togounoffice.com
- ubagroupsggh.com
- un-unicef.org
- unicomba.com
- universalcoba.com



:SHA-1

- 0450aaf8ed309ca6baf303837701b5b23aac6f05
- bb909d9c27a509bf97cdc85268556ff5a6d2550a
- f325970fd24bb088f1befdae5788152329e26bf3
- a351842ee01374d66bae35354ffe72f0b1b8a40b

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

המידע המובא לעיל לוקט ועובד על ידי CERT-IL במטרה לספק ידע רלוונטי ואקטואלי לעוסקים בתחום ההגנה בסייבר לטובת השכלה וידע כללי. אין במידע זה 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.