



בלמ"ס

לבן :TLP

- 1 -

13/05/2017

י"ג אדר תשע"ז

סימוכין : ב-ס-160

ארוע "חץ וקשת" - הנחיות התמודדות עם כופרת WannaCry

תקציר

ביום שישי ה-12 במאי זוהה גל התקפות כופרה מאסיבי כנגד עשרות אלפי מחשבים בארגונים רבים ובעשרות מדינות ברחבי העולם, ביניהם Telefonica בספרד, שירות הבריאות הלאומי בבריטניה ו-FedEx בארה"ב. התקיפה מנצלת חולשת אבטחה אשר פורסמה בהדלפות Shadow Broker במהלך חודש שעבר.

פרטים

ביממה האחרונה זוהו מתקפות כופרה מאסיביות במספר מדינות באירופה בהן ספרד, בריטניה ופורטוגל באמצעות פוגען כופר ממשפחת WannaCry. נראה כי התקיפה מנצלת מספר חולשות אבטחה ידועות, אחת מהן פורסמה בהדלפה של Shadow Broker במהלך אפריל (מדובר על פגיעות מוכרת של חברת מיקרוסופט, MS17-010, שתוקנה במרץ 2017 וכולל פגיעות בפרוטוקול SMB¹).

דיווחים רבים אודות המתקפה והשפעותיה התקבלו ממספר בתי חולים ברחבי בריטניה. תקיפות אלו גרמו, בין השאר, להשבתת הפעילות באותם בתי חולים ולהפרעה בטיפול בחולים. בנוסף, מתקפת הכופרה בספרד הובילה לפגיעה משמעותית בחברת התקשורת הענקית "Telefónica".

תוכנת הכופר מגיעה למחשבי המשתמשים באמצעות הודעת דוא"ל עם קובץ מצורף. פתיחת הקובץ על ידי המשתמש, מפעילה את תהליך ההתקנה וההתפשטות של תוכנת הכופר. בעת ההפעלה, מבצעת תוכנת הכופר סריקה של כתובות בתוך הרשת הפנימית של הארגון וגם בטווח כתובות רנדומאלי באינטרנט לטובת חיפוש אחר מחשבים פגיעים לחולשת שירות שיתוף הקבצים של מיקרוסופט בגרסה SMB v1.

תוכנת הכופר סורקת את תיקיות המחשב ומצפינה את רוב סוגי הקבצים השימושיים. לאחר ההצפנה, התוכנה מציגה הודעה הדורשת מהמשתמש לשלם עבור פתיחת ההצפנה סכום של בין 300-600 דולרים. תרשים א' מציג מסך לדוגמא בו נדרש מהמשתמש תשלום הכופר. פרטים נוספים נמצאים עדיין בחקירה,

¹ <https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html>



בלמיס

לבן :TLP

- 2 -

ויתעדכנו עם המשך החקירה. רשימת מערכות ההפעלה הפגיעות לסוג זה של תוכנת כופרה מפורטת בנספח א'.



תרשים א': צילום מסך של הודעת הכופרה לאחר הצפנת הקבצים



בלמיס

TLP: לבן

- 3 -

להלן אוסף פעולות לביצוע:

מנהלי

- יש להוציא הודעה לעובדים בארגון להעלאת מודעות לזיהוי דוא"ל חשוד עוד לפני תחילת שבוע העבודה הקרוב. מצורפת המלצה לנוסח לעדכון עובדים (מצ"ב נספח ב').
- יש להיערך עם צוותי תגובה לקראת אפשרות להידבקות והתפשטות ביום ראשון.

טכני

- מומלץ לא לחסום את התעבורה לכתובת
www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea[.]com
- עדכון גרסה אחרונה ועדכנית של תוכנת האנטי וירוס בעמדות הקצה והשרתים. מצורף נספח ג' המפרט את הגרסאות והעדכונים.
- יש לוודא ב-Firewall כי שירותי SMB לא נגישים מהאינטרנט (פורטים TCP 139, 445 ו-UDP 137, 138).
- אם מותקן רכיב SNORT יש לצרף את החוק המפורט בנספח ד'.
- יש לעדכן את מערכות ההפעלה בארגון
א. התקנת עדכון MS-17-010 :
<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>
ב. התקנת עדכון MS-17-010 למערכות אשר אינן נתמכות יותר כמו חלונות XP ו-Windows Server 2003 :
<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks>
- יש לעדכן מערכות ההגנה והניטור באינדיקטורים המופיעים בקובץ האקסל המצורף. כמו כן יש להוסיף את חוקי YARA במערכות הרלוונטיות (ראה נספח ה').
- במידה וקיימת מערכת הלבנה יש לוודא יישום הגדרת Reconstruction במערכות הסינון וההלבנה לקבלת דוא"ל המכיל צרופות מסוג Office.
- בנספח ו' מצורף חוק לניטור שינויים רלוונטיים ב-Registry של עמדת הקצה שניתן להפעילו ב-GPO הארגוני.
- יש לבחון ניטור שינויי קבצים במערכות הקצה ובשרתי הקבצים לניטור שינויי סיומות קבצים לסיומת "WNCRY". ניטור זה מהווה אינדיקציה לקבצים שהוצפנו.
- במידה וניתן יש לחסום שירותי SMB v1 בשרתים ובתחנות קצה בארגון.
- מצורף קובץ אינדיקטורים (IoC).
- ממשל זמין בשיתוף עם רשות הסייבר הקימו אתר להורדת עדכונים חיוניים להתמודדות עם האירוע. היכנסו לקישור

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.



בלמיס

TLP: לבן

- 4 -

בברכה,

CERT-IL

טל: 072-3990800

team@cert.gov.il

נספח א' – מערכות הפעלה הפגיעות לתוכנת הכופרה

א. Microsoft Windows Vista SP2

ב. Windows Server 2008 SP2 and R2 SP1

ג. Windows 7

ד. Windows 8.1

ה. Windows RT 8.1

ו. Windows Server 2012 and R2

ז. Windows 10

ח. Windows Server 2016

נספח ב' – טיוטא להודעה בארגון

במהלך סוף השבוע בוצעה מתקפה רחבת היקף של פוגענים מסוג תוכנות כופר כנגד ארגונים שונים ברחבי העולם. הפוגענים הגיעו בצורת קישור או בצורת צרופה. פתיחת הצרופה מתחילה את תהליך הצפנת קבצים והתפשטות הפוגען ברשת הארגונית.

יכולות ההתפשטות והדבקת מחשבים ושרתים ברשת המקומית של פוגען זה מהירות וקשות לעצירה, ולכן כמות הנדבקים בעולם הינה גדולה באופן חריג.

מחלקת/אגף הגנת הסייבר _____ ביצעו פעולות לזיהוי, חסימה והתראה על פוגענים מסוג זה, כל זאת בכדי למנוע את חדירתם לארגונו.

בכדי לחזק את מנגנוני ההגנה נדרשת גם תשומת הלב שלכם.

שים לב!

א. לא לפתוח צרופות ממקור לא ידוע.



בלמיס

לבן :TLP

- 5 -

ב. לא ללחוץ על לינקים ממקור לא ידוע או חשוד.

ג. במידה ויש לך חשש כי נתקפת – אל תהסס, תוכל לדווח ל – צוות ה _____ SOC - או טלפון :
 XXXXXX באופן מיידי.

תודה על שיתוף הפעולה,

נספח ג'

מוצר	סוג מוצר	גרסה	מועד עדכון אחרון	קישור להגדרות	וקטור כניסה	חולשה
IBM XGS	Next Gen IPS	Version 5 and up	11 למאי 2017	https://exchange.xforce.ibmcloud.com/collection/WCry2-Ransomware-Outbreak-8b186bc4459380a5606c322ee20c7729		מונע
IBM BigFix	End point , server Patch mgmt and therat prevention	EDR Version				מונע
Microsoft	מערכת הפעלה	ומעלה XP				מונע
Mcafee	EPO	ExtraDat		https://kc.mcafee.com/corporate/index?page=content&id=KB89335		מונע
Kaspersky	IPS					מונע
Symantec h	IPS			זיהוי חולשה		מונע
Fireeye	HX, NX, EX					מונע
Trend Micro	Deep Security	כול הגרסאות	מאפריל	https://success.trendmicro.com/solution/1117391		מונע



בלמיס

TLP: לבן

- 6 -

	מונע	https://success.trendmicro.com/solution/1117391	מאפרייל	כול הגרסאות	Tipping Point IPS	Trend Micro
	מונע	https://success.trendmicro.com/solution/1117391	מאפרייל	כול הגרסאות	Vulnerability protection	Trend Micro
	מונע	https://success.trendmicro.com/solution/1117391	12.05		OSCE 11	Trend Micro
זיהוי בלבד	זיהוי בלבד	https://success.trendmicro.com/solution/1117391	מאפרייל	כול הגרסאות	DDI	Trend Micro
	מונע	https://success.trendmicro.com/solution/1117391	איו צורך מזהה ע"י Machine Learning		OSCE XG	Trend Micro
					IPS	Checkpoint
			12.5		Anti-Bot, Anti-Virus	Checkpoint
			20-Apr		IPS	Checkpoint
	מונע	https://www.carbonblack.com/2017/05/13/protect-organization-wannacry-ransomware/				Carbon Black
	מונע				Agent	Cynet
	מונע				Agent	Secdo
	מונע	דואר נכנס		החל מגרסא 7.8	Email security	Forcepoint
	מונע	גלישה לאתרים ותקשורת עם C&C		החל מגרסא 7.8	Web Security	Forcepoint



בלמי"ס

לבן :TLP

- 7 -

מונע	https://kc.mcafee.com/corporate/index?page=content&id=KB89335&t	-13 May-17	ExtraDat	ePO (ENS)	McAfee
מונע	https://kc.mcafee.com/corporate/index?page=content&id=KB89335&t		Access Protection	ePO (ENS)	
מונע	ftp://custftp2.nai.com/Outgoing/Shimon/UDS-05122017.zip	-13 May-17		NSP (IPS)	
מונע		-13 May-17		McAfee Web Gateway	

נספח ד' – חוק SNORT

```
alert tcp $HOME_NET 445 -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:2;)
```

נספח ה' – חוק YARA

```
rule wannacry_1 : ransom
{
    meta:
        author = "Joshua Cannell"
        description = "WannaCry Ransomware strings"
        weight = 100
        date = "2017-05-12"

    Strings:
        $s1 = "Ooops, your files have been encrypted!" wide ascii nocase
        $s2 = "Wanna Decryptor" wide ascii nocase
        $s3 = ".wcry" wide ascii nocase
        $s4 = "WANNACRY" wide ascii nocase
```



בלמי"ס

לבן :TLP

- 8 -

\$s5 = "WANACRY!" wide ascii nocase
\$s7 = "icacIs . /grant Everyone:F /T /C /Q" wide ascii nocase

```
Condition:  
any of them  
}  
rule wannacry_2{  
meta:  
author = "Harold Ogden"  
description = "WannaCry Ransomware Strings"  
date = "2017-05-12"  
weight = 100  
strings:  
$string1 = "msg/m_bulgarian.wnry"  
$string2 = "msg/m_chinese (simplified).wnry"  
$string3 = "msg/m_chinese (traditional).wnry"  
$string4 = "msg/m_croatian.wnry"  
$string5 = "msg/m_czech.wnry"  
$string6 = "msg/m_danish.wnry"  
$string7 = "msg/m_dutch.wnry"  
$string8 = "msg/m_english.wnry"  
$string9 = "msg/m_filipino.wnry"  
$string10 = "msg/m_finnish.wnry"  
$string11 = "msg/m_french.wnry"  
$string12 = "msg/m_german.wnry"  
$string13 = "msg/m_greek.wnry"  
$string14 = "msg/m_indonesian.wnry"  
$string15 = "msg/m_italian.wnry"  
$string16 = "msg/m_japanese.wnry"  
$string17 = "msg/m_korean.wnry"  
$string18 = "msg/m_latvian.wnry"  
$string19 = "msg/m_norwegian.wnry"  
$string20 = "msg/m_polish.wnry"  
$string21 = "msg/m_portuguese.wnry"  
$string22 = "msg/m_romanian.wnry"  
$string23 = "msg/m_russian.wnry"  
$string24 = "msg/m_slovak.wnry"  
$string25 = "msg/m_spanish.wnry"  
$string26 = "msg/m_swedish.wnry"  
$string27 = "msg/m_turkish.wnry"  
$string28 = "msg/m_vietnamese.wnry"  
condition:  
any of ($string*)  
}
```

נספח ו'

מצי"ב קובץ הנחיות מחברת מקאפי למימוש ההגנה על ערכי ה Registry והתראה על שימוש

<https://kc.mcafee.com/corporate/index?page=content&id=KB89335>

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר



בלמי"ס

TLP: לבן

- 9 -