משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר

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

13/05/2017
י"ז באייר תשע"ז
סימוכין: ב-ס-160

אירוע "חץ וקשת" - הנחיות התמודדות עם כופרת WannaCry

(מעודכן נכון ל-14/05/2017 בשעה 11:45)

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 SMB[1] .

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 התקשרות 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.

[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

תרשים א' מציג מסך לדוגמא בו נדרש מהמשתמש תשלום הכופר. פרטים נוספים נמצאים עדיין בחקירה, 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

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

להלן אוסף פעולות לביצוע:

מנהלי

1. 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').
2. יש להיערך עם צוותי תגובה לקראת אפשרות להידבקות והתפשטות ביום ראשון.

טכני

1. מומלץ לא לחסום את התעבורה לכתובת www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com.
2. אם ארגונכם עושה שימוש בשרת פרוקסי, יש להגדיר את הדומיין הנ"ל ברשימת ה- BYPASS של הפרוקסי עבור כלל התחנות.
3. עדכון גרסה אחרונה ועדכנית של תוכנת האנטי וירוס בעמדות הקצה והשרתים. מצורף נספח ג' המפרט את הגרסאות והעדכונים.
4. יש לוודא ב- Firewall כי שירותי SMB לא נגישים מהאינטרנט (פורטים TCP 445, 139 ו- UDP 137, 138).
5. מומלץ לוודא כי שרתי Terminal Services ארגוניים אינם נגישים ישירות מרשת האינטרנט (פורט 3389) אלא רק דרך שירותי VPN עם הזדהות מתאימה.
6. אם מותקן רכיב SNORT יש לצרף את החוק המפורט בנספח ד'.
7. 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/
8. יש לעדכן מערכות ההגנה והניטור באינדיקטורים המופיעים בקובץ האקסל המצורף. כמו כן יש להוסיף את חוקי YARA במערכות הרלוונטיות (ראה נספח ה').
9. במידה וקיימת מערכת הלבנה יש לוודא יישום הגדרת Reconstruction במערכות הסינון וההלבנה לקבלת דוא"ל המכיל צרופות מסוג Office.
10. בנספח ו' מצורף חוק לניטור שינוים רלוונטיים ב-Registry של עמדת הקצה שניתן להפעילו ב- GPO הארגוני.
11. יש לבחון ניטור שינויי קבצים במערכות הקצה ובשרתי הקבצים לניטור שינוי סיומות קבצים לסיומת "WNCRY". ניטור זה מהווה אינדיקציה לקבצים שהוצפנו.
12. במידה וניתן יש לחסום שירותי SMB v1 בשרתים ובתחנות קצה בארגון.
13. מצורף קובץ אינדיקטורים (IoC).
14. ממשל זמין בשיתוף עם רשות הסייבר הקימו אתר להורדת עדכונים חיוניים להתמודדות עם האירוע. היכנסו לקישור

15. ה-cert הספרדי פרסם כלי ייעודי לתחנת קצה המשמש למניעת הדבקה של wannacry החדש על ידי החדרת ה-mutex שלו למערכת. הכלי דורש הפעלה מחדש לאחר restart. לפרטים נוספים לחצו כאן.

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: 072-3990800

team@cert.gov.il

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

בלמ"ס

TLP: **לבן**

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 לארגוננו.

בכדי לחזק את מנגנוני ההגנה נדרשת גם תשומת הלב שלכם.

שים לב!

א. לא לפתוח צרופות ממקור לא ידוע.

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",

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

בלמ"ס

TLP: **לבן**

נספח ג' – רשימת מוצרים לסיוע בהתמודדות מול הנוזקות

מוצר	סוג מוצר	גרסה	מועד עדכון אחרון	קישור להגדרות	וקטור כניסה	חולשה
McAfee	ePO (ENS)	ExtraDat	May--13 17	https://kc.mcafee.com/corporate/index?page=content&id=KB89335		**מונע**
	ePO (ENS)	Access Protection		https://kc.mcafee.com/corporate/index?page=content&id=KB89335		**מונע**
	NSP (IPS)		May--13 17	ftp://custftp2.nai.com/Outgoing/Shimon/UDS-05122017.zip		**מונע**
	McAfee Web Gateway		May--13 17			**מונע**
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	XP ומעלה				מונע
Kaspersky	IPS					מונע
Symantec	חתימות	[SID 29064] System Infected: Ransom.Ransom32 Activity [SID 23875] OS Attack: Microsoft SMB MS17-010 Disclosure Attempt [SID 23737] Attack: Shellcode Download Activity				
Symantec	IPS	LiveUpdate definitions version 20170512.009		זיהוי חולשה		מונע

Fireeye	HX, NX, EX				מונע	מונע
Trend Micro	Deep Security	כול הגרסאות	מאפריל	https://success.trendmicro.com/solution/1117391	מונע	מונע
Trend Micro	Tipping Point IPS	כול הגרסאות	מאפריל	https://success.trendmicro.com/solution/1117391	מונע	
Trend Micro	Vulnerability protection	כול הגרסאות	מאפריל	https://success.trendmicro.com/solution/1117391	מונע	מונע
Trend Micro	OSCE 11		12.05	https://success.trendmicro.com/solution/1117391	מונע	
Trend Micro	DDI	כול הגרסאות	מאפריל	https://success.trendmicro.com/solution/1117391	זיהוי בלבד	זיהוי בלבד
Trend Micro	OSCE XG		איו צורך מזוה ע"י Machine Learning	https://success.trendmicro.com/solution/1117391	מונע	מונע
Checkpoint	IPS			http://blog.checkpoint.com/2017/05/12/global-outbreak-wanacryptor/		מונע
Checkpoint	Anti-Virus		12.5			מונע
Checkpoint	Anti-Bot		12.5			זיהוי בלבד
Checkpoint	SandBlast		20-Apr		מונע	
Carbon Black				https://www.carbonblack.com/2017/05/13/protect-organization-wannacry-ransomware/		מונע
Cynet	Agent					מונע
Secdo	Agent					מונע
Forcepoint	Email security	החל מגרסא 7.8			דואר נכנס	מונע

Forcepoint	Web Security	החל מגרסא 7.8			גלישה לאתרים ותקשורת עם C&C	מונע
NYOTRON PARANOID		ALL VERSIONS (NO UPDATES REQUIRED)		https://nyotron.com/wannacry-ransomware-cyberattack-impacts-organizations-worldwide/		מונע

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
$s5 = "WANACRY!" wide ascii nocase
$s7 = "icacls . /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'

מצ"ב קובץ הנחיות מחברת מקאפי למימוש ההגנה על ערכי ה Registry והתראה על שימושן

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