10 במאי 2015

כ"א באייר תשע"ה

עדכון אחרון 10 בנובמבר 2015

סימוכין: ל-ס-098

התמודדות עם נוזקת כופר (Ransomware)

נוזקת כופר[1] הינה תוכנה פוגענית המופצת ונשלטת על ידי קבוצות פשיעה למיניהן. לאחר חדירתה והתקנתה מצפינה הנוזקה את תכולת הדיסק (קבצי נתונים שונים כמו מסמכי WORD, EXCEL, תמונות ועוד), ומציגה הודעת דרישה לתשלום כופר כספי (לרוב באמצעות תשלום במטבע הווירטואלי - Bitcoin[2]), על מנת לשחרר את ההצפנה ולאפשר שוב את הגישה לקבצים.

תופעת תוכנות הכופר אינה חדשה, אולם ישנה עלייה משמעותית בכמות השימוש בה. מיליוני מחשבי אנשים פרטיים, ומחשבי משתמשים בארגונים נפגעו מאיום זה ונאלצו לשלם את דמי הכופר או להתקין את המחשבים מחדש, לעיתים תוך כדי איבוד מידע משמעותי ורב ערך עבורם.

בעולם נפוצו מספר גרסאות של נוזקות כופר כדוגמת: Cryptolocker, CTB-Locker, PrisonLocker, Cryptowall, CoinVault, Teslacrypt ועוד, אולם לכולם ישנו מכנה משותף והוא: הנדסת אנוש!

היכולת לשכנע אנשים ללחוץ על קישורים בדואר האלקטרוני על מנת לאפשר את התקנתה של התוכנה הזדונית. אולם גם אנטי-וירוס שאינו מעודכן או כלל לא מותקן, מערכת הפעלה ותוכנות שלא עודכנו בעדכוני האבטחה המופצים יאפשרו התקנתה של הנוזקה במחשבים רבים.

---

[1] Israel Defense – תוכנת כופר
[2] Bitcoin - ויקיפדיה

מרביתן של נוזקות הכופר מגיעות באמצעות דואר האלקטרוני, ספאם או ממוקד אישית (Spear Phishing). דרך נוספת מוכרת לחדירת הנוזקה למחשב היא באמצעות פרוטוקול RDP[3] (Remote desktop protocol) במחשבי Windows כאשר הפורט[4] של הפרוטוקול 3389 מאופשר לגישה מהאינטרנט למחשב האישי\ארגוני.

מרגע שהנתונים בדיסק הוצפנו, רק לתוקף יש את היכולת (מפתח ההצפנה) לשחרור ההצפנה.

<u>תופעות בעת הדבקה בנוזקת כופר:</u>

- מניעת כניסה למערכת ההפעלה Windows.
- הצפנת הקבצים בדיסק, כך שלא יהיה ניתן להשתמש בהם.
- עצירת יכולתן של תוכנות מסוימות מלרוץ במחשב, כגון דפדפנים (Firefox, IE, chrome, וכדומה).
- הצגת הודעת דרישת תשלום דמי כופר

<u>דרכים לצמצום הידבקות בנוזקת כופר במחשב הביתי ובמחשב אירגוני:</u>

1. חשוב לוודא כי מערכת ההפעלה והתוכנות המותקנות במחשב הן בגרסתן האחרונה ומעודכנות בכל עדכוני האבטחה שפורסמו. לבדוק במערכת ההפעלה שמצב עדכון אוטומטי[5] מופעל.
2. להתקין תוכנת אנטי-וירוס[6] הכוללת מנגנונים של מוניטין ובדיקות היוריסטיות[7] (רוב תוכנות אנטי-וירוס מכילות רכיבים אלו כולל הגנה על הדפדפנים).
3. להשתמש בדפדפנים[8] בגרסתם האחרונה שהיצרן ממליץ עליה.
4. להימנע מלחיצה על קישורים בדואר האלקטרוני.
5. לבדוק סיומות קבצים המגיעים בצרופות(Attachments). יש למחוק קבצי הפעלה[9] עם סיומות כדוגמת CAB, MSI,EXE, BAT ועוד, ולא לאפשר את כניסתם למערכת (נדגיש כי צורת הצלמית (icon) של הקובץ אינה מעידה בהכרח על סוג הקובץ).
6. טרם שמקליקים חושבים! לא פותחים קבצי צרופה לפני שבודקים! האם השולח מוכר או לא? לבחון היטב את נושא ההודעה, האם הנושא רלוונטי? האם הוא קשור לשולח? האם ההודעה קשורה לשיח

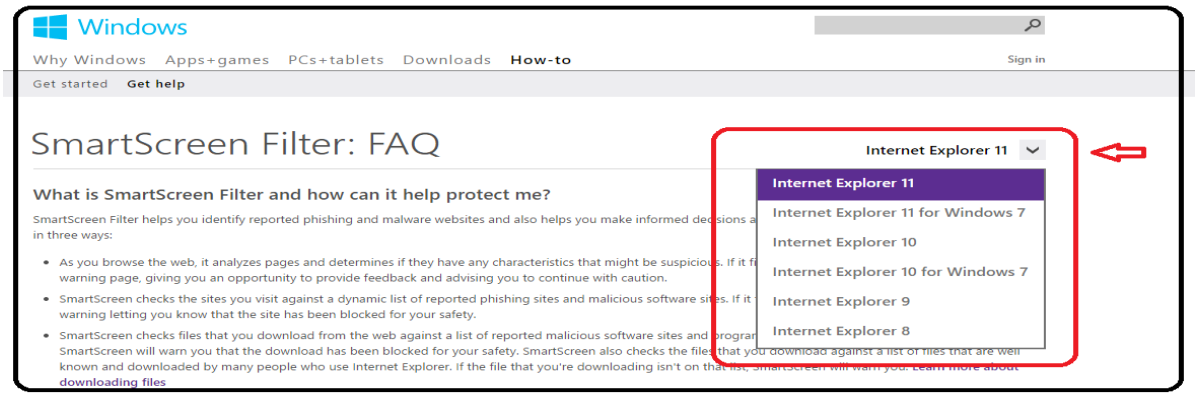
---

[3] נטרול RDP – Microsoft: Enable or disable Remote Desktop
[4] פורט (PORT) – ויקיפדיה
[5] הפעלה או ביטול של העדכון האוטומטי ב- Windows 7 , Windows Update - Windows Help
[6] לרשימת תוכנות אנטי-וירוס חינמיות באתר CERT-IL
[7] מהו מנגנון היוריסטי - ESET
[8] לרשימת דפדפנים באתר CERT-IL
[9] רשימת קבצים עם סיומות מסוכנות File-Extantions.org - Dangerous and malicious file extension list

המשותף ביניכם? האם ציפיתם לקובץ? לפיכך יש לנקוט בגישה: במידה ויש ספק – אין ספק! פשוט לא פותחים!

7. התקנת תוספים לדפדפנים מסוג Pop-Up Blocker[10] יצמצם באופן ניכר את קפיצתם של חלוניות פרסום Adware[11] שעשויות להיות נגועות בפוגענים בעת גלישה באתרים.
8. חברת מיקרוסופט שילבה בדפדפן Internet Explorer את אופציית Smart-Screen (מומלץ להשתמש בגרסת הדפדפן האחרונה) שיכולה לסייע בצמצום המקרים הבאים:
   - Anti-Phishing[12]
   - Application reputation[13]
   - Anti-Malware protection[14]

להלן קישור לדף הסבר על התכונה: Windows SmartScreen Filter ראה איור 1. לבחירת גרסת הדפדפן.



Smartscreen Filter .1 איור

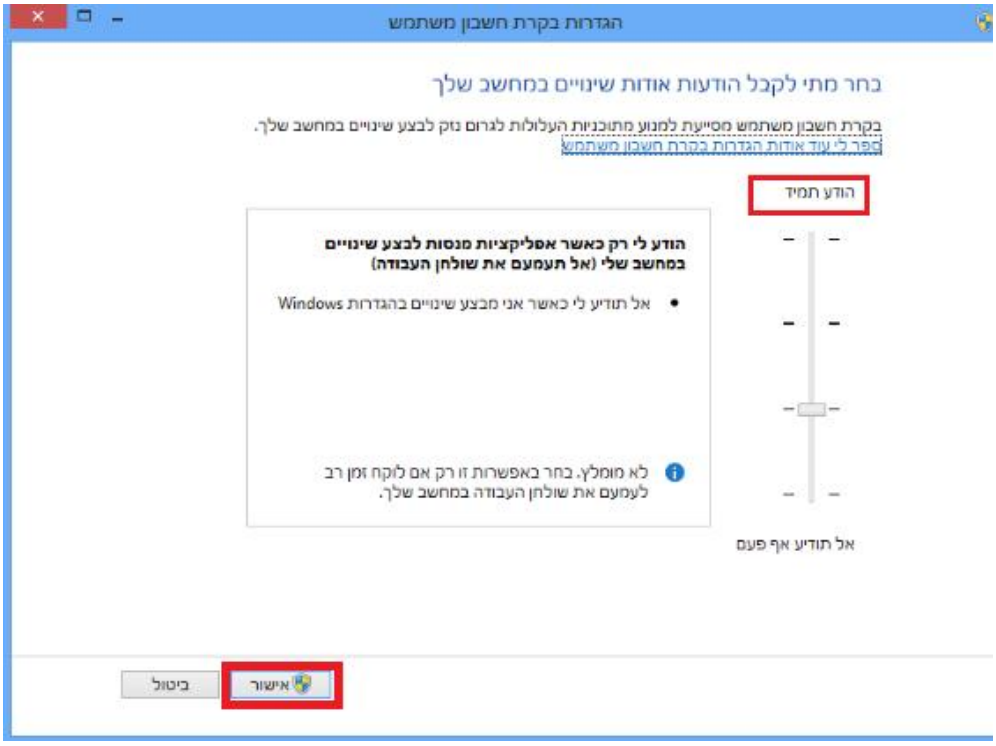
9. לבצע גיבוי קבוע ומסודר לקבצים חשובים (מידע, תמונות או כל קובץ חשוב אחר), להתקן חיצוני (דיסק קשיח חיצוני, כונן USB, מדיה אופטית), או לענן ציבורי[15] חינמי[16] או בתשלום. מיקרוסופט שילבה החל במערכת הפעלה Windows 8.1 ומעלה, מנגנון מובנה לגיבוי בענן Microsoft בשם

[10] Pop-Up Blocker in Safari ,Opera pop-ups ,privacy settings for IE ,Firefox Pop-up settings ,pop-ups in Chrome
[11] תוכנת פרסום Adware - ויקיפדיה
[12] דיוג(Phising) - ויקיפדיה
[13] SmartScreen Application Reputation
[14] הערה: תוכנות Anti-Malware אינן מחליפות את תוכנת האנטי-וירוס אלא משמשות כמוצר הגנה משלים.
[15] מחשוב ענן – ויקיפדיה
[16] לדוגמה, רשימת חברות המעניקות שרותי ענן חינם about.com – 33 Free Cloud Storage Services

Microsoft One Drive[17]. גם אתרים רבים אחרים מעניקים שרות גיבוי חינם בענן, בנפח התחלתי מסוים, להגדלת נפח השירות יידרש תשלום בהתאם.

10. העלאת רמת האבטחה של מנגנון UAC(User Access Control).

להגדרת ה-UAC של Win7 בחר: לוח בקרה – מערכות ואבטחה- מרכז פעילות-תחת מרכז הפעלות לחץ על "שנה הגדרות של בקרת חשבון משתמש", בחלון שיפתח העלה את המחוג כלפי מעלה לכיוון "הודע תמיד" ולחץ אישור (איור 2).

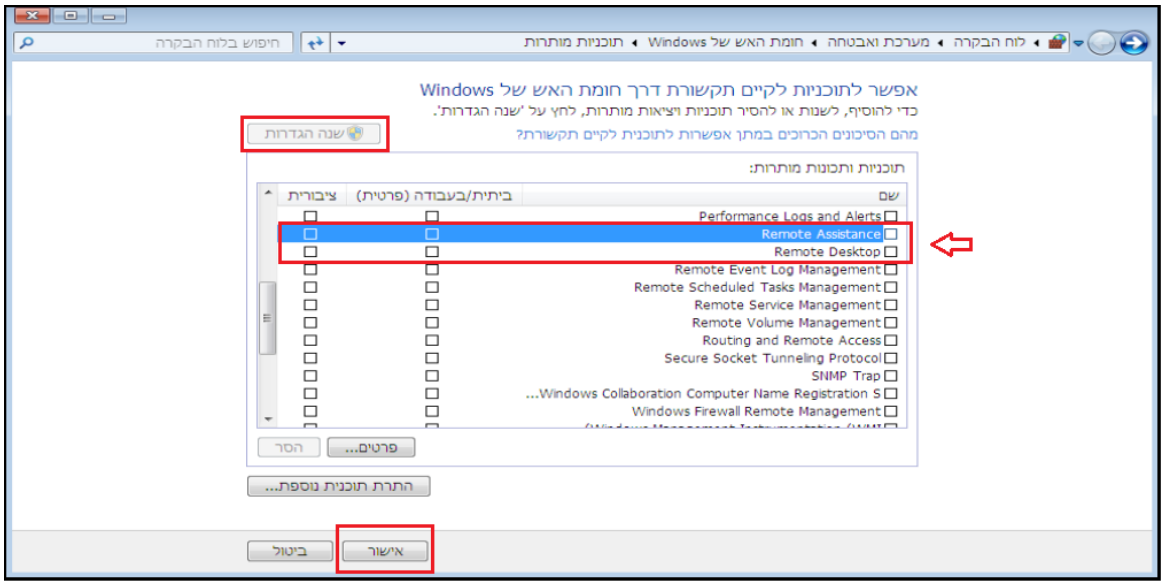


איור 2. WIN7 UAC

11. לחסום את פורט 3389 (RDP) באמצעות ה- FW הפנימי במחשב ואם ניתן גם בנתב החיצוני לכניסה מהאינטרנט.

[17] מדריך לעבודה עם OneDrive

להגדרה הFW הפנימי של Win7 בחר: לוח בקרה – מערכת ואבטחה – אפשר תוכנית דרך חומת האש של Windows – בחר בלשונית שנה הגדרות, גלול את הרשימה והסר את ה-V מהאפשרויות Remote Assistance ו - Remote Desktop. לסיום הקלק על אישור (איור 3).



איור 3. WIN7 FW

<u>דרכים נוספות למזעור הסיכוי להדבקה בנוזקת כופר (בגרסאות שונות) ברשת האירגונית:</u>

ניתן לשקול בהתאמה לאופי הארגון מספר צעדים:

1. בדיקה כי מערכות ה- Mail Relay מעודכנות באופן תדיר בקובץ החתימות האחרון של יצרן התוכנה.
2. לחסום את תעבורת קבצי (ZIP/RAR) המכילים קבצי הרצה (Executables).
3. הפעלת בקרות להקטנת היכולת לפגיעת סייבר בארגון, לדוגמה באמצעות הפעלת EMET כלי מובנה חינמי של מיקרוסופט. לפרוט בקרה זו ובקרות מומלצות נוספות ניתן להוריד את המסמך "המלצות להפחתת חדירות סייבר לארגונים - גרסה מלאה גרסה 1.0 יוני 2015" מאתר ה-CERT.

4. הגדרת מדיניות (GPO) למניעת הרצה של Binaries מהספריות הבאות:

- `%appdata%\*.exe`
- `%appdata%\*\*.exe`
- `%localappdata%\*.exe`
- `%localappdata%\*\*.exe`

5. למנוע הרצה של Binaries על ידי הגדרה של SRP – Software Restriction Policy .

להלן מספר חוקי SRP הניתנים ליישום:

Block CryptoLocker executable in `%AppData%`

Path: `%AppData%\*.exe`

Security Level: Disallowed Description: Don't allow executable to run from `%AppData.%`

Block CryptoLocker executable in `%LocalAppData.%`

Path if using Windows XP: `%UserProfile%\Local Settings\*.exe`

Path if using Windows Vista/7/8: `%LocalAppData%\*.exe`

Security Level: Disallowed Description: Don't allow executable to run from %AppData.%

Block executable run from archive attachments opened with WinRAR:

Path if using Windows XP: `%UserProfile%\Local Settings\Temp\Rar*\*.exe`

Path if using Windows Vista/7/8: `%LocalAppData%\Temp\Rar*\*.exe`

Security Level: Disallowed Description: Block executables run from archive attachments opened with WinRAR.

Block executable run from archive attachments opened with 7zip:

Path if using Windows XP: `%UserProfile%\Local Settings\Temp\7z*\*.exe`

Path if using Windows Vista/7/8: `%LocalAppData%\Temp\7z*\*.exe`

Security Level: Disallowed Description: Block executables run from archive attachments opened with 7zip.

Block executable run from archive attachments opened with WinZip: Path if using Windows XP: `%UserProfile%\Local Settings\Temp\wz*\*.exe`

Path if using Windows Vista/7/8: `%LocalAppData%\Temp\wz*\*.exe` Security Level: Disallowed Description: Block executables run from archive attachments opened with WinZip.

Block executable run from archive attachments opened using Windows built-in Zip support:

Path if using Windows XP: `%UserProfile%\Local Settings\Temp\*.zip\*.exe`

Path if using Windows Vista/7/8: `%LocalAppData%\Temp\*.zip\*.exe` Security Level: Disallowed Description: Block executables run from archive attachments opened using Windows built-in Zip support.

<u>פעולות אפשריות במידה ועולה החשש לפגיעה או לאחר שהמחשב נפגע והוצגה בקשת כופר</u>

במחשב ביתי:

1. לא לכבות את המחשב
2. לנתק את המחשב מהאינטרנט
3. לנסות ולבצע שיחזור גרסאות קודמות לקבצים במערכת ההפעלה לתאריך שלפני ההדבקה, אם כי קיים סיכוי קלוש שפעולה זו תעזור במידה ולא בוצעה העלאה של רמת ה-UAC (כפי שמתואר בסעיף 10 לצמצום הדבקות בנוזקת כופר), מאחר ולנוזקות הכופר בגרסאותיהם החדשות ישנה היכולת לנטרל ולפגוע ביכולת השחזור, אולם עדיין שווה לנסות.
4. לנסות ולבצע שיחזור מערכת[18] (System restore) למערכת ההפעלה לתאריך שלפני ההדבקה, אם כי קיים סיכוי קלוש שפעולה זו תעזור במידה ולא בוצעה העלאה של רמת ה-UAC (כפי שמתואר בסעיף

[18] שיחזור מערכת Windows

10 לצמצום הדבקות בנוזקת כופר), מאחר ולנוזקות הכופר בגרסאותיהם החדשות ישנה היכולת לנטרל ולפגוע ביכולת השחזור, אולם עדיין שווה לנסות.

5. במידה ולא ניתן לבצע שיחזור מערכת, אך ידוע בוודאות כי קיים גיבוי לקבצים החשובים, ניתן בלית ברירה לפרמט ולהתקין את מערכת ההפעלה מחדש ולשחזר את הנתונים מהגיבוי החיצוני או מהענן.

ברשת אירגונית:

בעזרתו של איש מקצוע מיומן לצורך חקירה וניתוח של הראיות ניתן לבצע את הפעולות הבאות:

1. לא לכבות את המחשב
2. לנתק מיד את המחשב מהרשת
3. ליצור העתק (Forensics Image) של הדיסק הקשיח וזיכרון ה RAM של המחשב הנגוע
4. לאסוף ולשמור (ברשת אירגונית) את הלוגים של Firewall, IPS, AD, Local System logs
5. לשמור את קבצי ה pcap's של תעבורת הרשת במידה וקיימים.
6. במידה וקיים Volume Shadow Copy (VSC) ניתן לנסות לבצע שיחזור לעותק קודם. להסבר: vssadmin. ניתן לעשות שימוש ב- shadow explorer ולנסות לשחזר את ה- VSC Snapshots, אם כי כבר נצפו סוגים שונים של נוזקות כופר אשר מחפשות ומוחקות את ה- VSC Snapshots.

IOC

מיקום ה- binaries של ה- Malware

```
%AppData%\<Random>.exe

%LocalAppData%\<random>.exe
```

במידה והנוזקה כבר רצה על התחנה יופיעו אחד או יותר מערכי ה- registry הבאים:

- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "variant name"`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "Variant name_<version"<`

- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*Variant"`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "<Random"<`

<u>זיהוי תהליך ההצפנה על תחנת הקצה</u>

ניתן לעשות שימוש בסקריפט PowerShell על מנת לזהות קבצים שעוברים תהליך הצפנה.

לביצוע, הפעל PowerShell Console עם הרשאות Administrator והרץ את הקוד הבא:

```
(Get-Item HKCU:\Software\CryptoLocker\Files).
GetValueNames().
Replace("?","\") | Out-File CryptoLockerFiles.txt -Encoding
Unicode
```

<u>הבהרה</u>

לכל נוזקת כופר ישנן גרסאות שונות אשר פועלות בדרכים שונות. בעוד גרסאות אחדות נראות דומות לגרסה מסוימת, לא בטוח כי הכלים המפורסמים בציבור יעזרו לפענח בהצלחה את קבצים המוצפנים ולהציל את המידע. זאת בגלל הבדלי גרסאות, עדכונים או סיבות אחרות. לפיכך טרם ביצוע כל פעולה או ניסיון תיקון באמצעות כלי כלשהו המתפרסם בציבור, יש לנקוט במשנה זהירות, להבין היטב את ההשלכות ולדעת כי לא תמיד ניתן יהיה לפענח את ההצפנה ולשחזר את הקבצים.

מידע נוסף:

- מדריך של חברת Kaspersky כיצד לנסות ולהסיר את הצפנת תוכנת הכופר "CoinVault" מהמחשב בקישור: https://noransom.kaspersky.com/static/CoinVault-decrypt-howto.pdf

- כלי חינמי לפרימת הנוזקה "ransomware decryptor" של חברת Kaspersky בקישור: https://noransom.kaspersky.com

- הסבר של חברת FireEye לנוזקת Cryptolocker עם מידע שעשוי להועיל, בקישור: https://www.fireeye.com/blog/executive-perspective/2014/08/your-locker-of-information-for-cryptolocker-decryption.html

- הסבר של חברת Cisco לנוזקת TeslaCrypt עם מידע וכלי שעשוי להועיל בקישור: http://blogs.cisco.com/security/talos/teslacrypt

- מדריך מידע ושאלות נפוצות לנוזקות TeslaCrypt ו- Alpha Crypt באתר bleepingcomputer בקישור: http://www.bleepingcomputer.com/virus-removal/teslacrypt-alphacrypt-ransomware-information

- להורדת כלי חינמי לפענוח הצפנה של נוזקת TeslaCrypt לקבצים .ECC , .EZZ , .EXX בקישור: http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/

- חברת Emsisoft הצליחה ליצור כלי לחילוץ קבצים אשר הוצפנו על ידי נוזקת הכופר Gomasom http://tmp.emsisoft.com/fw/decrypt_gomasom.exe