16 מרץ 2016

ו' אדר ב תשע"ו

סימוכין: ל-ס- 173

הנדון: התמודדות עם נוזקת כופר (Ransomware) ברשת הארגונית

נוזקת כופר הינה תוכנה פוגענית המופצת ונשלטת על ידי קבוצות פשיעה למיניהן. לאחר הדבקת מחשב הקורבן, מצפינה הנוזקה את תכולת הדיסק הקשיח של המשתמש (קבצי נתונים שונים כמו מסמכי WORD, EXCEL, תמונות וכדומה) ומציגה הודעת דרישה לתשלום כופר כספי (לרוב באמצעות המטבע הווירטואלי Bitcoin[1]), בתמורה לשחרור ההצפנה ופתיחת הגישה לקבצים.

הדרכים הנפוצות ביותר להפצת הנוזקה הן באמצעות דואר האלקטרוני, בין אם בתפוצה רחבה או ממוקדת (Spear Phishing), ובין אם באמצעות השתלת קוד JavaScript המנצל חולשות אבטחה שונות באתר אינטרנט זדוני או פגוע.

תופעת זו איננה חדשה, אולם בעת האחרונה חלה עלייה משמעותית בשכיחות התרחשותה ובמספר המשפחות הקיימות של נוזקות מסוג זה, בהן: Cryptolocker, CTB-Locker, PrisonLocker, Cryptowall, CoinVault ו-Teslacrypt. בחלק ממשפחות אלו ישנה יכולת לשחזר באופן עצמאי את מפתח ההצפנה ולפענח את הקבצים ואילו באחרות רק לתוקף עצמו יש את היכולת לשחרור ההצפנה.

מסמך זה סוקר דרכים המומלצות על ידי ה-CERT הלאומי לצמצום הסיכון להדבקות ולהתמודדות עם נוזקות כופר ברשת הארגונית.

[1] Bitcoin - ויקיפדיה

דרכים לצמצום הסיכון להדבקות בנוזקת כופר במחשבים ברשת הארגונית

1. חשוב לוודא כי מערכת ההפעלה והתוכנות המותקנות במחשב הן בגרסתן האחרונה ומעודכנות בעדכוני האבטחה האחרונים. מומלץ לוודא כי מצב העדכון האוטומטי[2] במערכת ההפעלה מופעל.
2. להתקין תוכנת אנטי-וירוס[3] הכוללת מנגנונים של מוניטין, הגנה על הדפדפנים ובדיקות היוריסטיות[4] (רוב תוכנות אנטי-וירוס מכילות רכיבים אלו).
3. מומלץ לחסום בשרת הדוא"ל הארגוני את אפשרות קבלתם של הודעות המכילות קבצי הפעלה,[5] כדוגמת קבצים בסיומת CAB, MSI, EXE, SCR וכדומה.
4. לנקוט בזהירות טרם לחיצה על צרופות קישורים המתקבלים בדואר האלקטרוני. מומלץ לוודא כי כתובת השולח אכן מוכרת, כי הקישור מפנה לאתר לגיטימי, כי ציפיתם לקובץ המצורף וכו'. יש לזכור כי הצלמית (Icon) של קובץ אינה מעידה בהכרח על סוגו.
5. הגדרת הדפדפן לחסימת חלונות קופצים[6] תצמצם באופן ניכר את קפיצתם של חלוניות פרסום שעשויות לשמש להדבקה בפוגענים בעת גלישה באתרים.
6. חברת מיקרוסופט שילבה בדפדפן Internet Explorer בגרסה 11 ואילך את אופציית Smart-Screen שיכולה לסייע בצמצום המקרים הבאים:
   - Anti-Phishing[7]
   - Application reputation[8]
   - Anti-Malware protection[9]

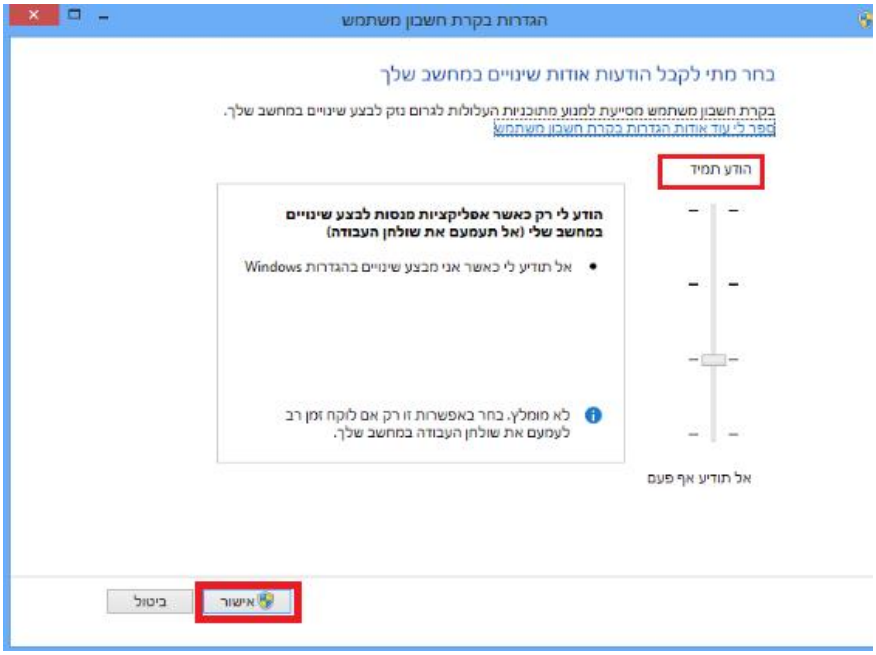
   להלן קישור לדף הסבר על התכונה: Windows SmartScreen Filter
7. לבצע גיבוי קבוע ומסודר לקבצים חשובים (מידע, תמונות או כל קובץ חשוב אחר), להתקן חיצוני (דיסק קשיח חיצוני, כונן USB, מדיה אופטית), או לענן ציבורי[10] חינמי[11] או בתשלום. Microsoft שילבה במערכת ההפעלה Windows 8.1 ומעלה, מנגנון מובנה לגיבוי בענן Microsoft One Drive[12]. אתרים רבים אחרים מעניקים שרות גיבוי חינם בענן, בנפח התחלתי כלשהו.

---

[2] הפעלה או ביטול של העדכון האוטומטי ב- Windows 7 , Windows Update - Windows Help
[3] לרשימת תוכנות אנטי-וירוס חינמיות באתר CERT-IL
[4] מהו מנגנון היוריסטי - ESET
[5] רשימת קבצים עם סיומות מסוכנות File-Extantions.org - Dangerous and malicious file extension list
[6] pop-ups in Chrome, Firefox Pop-up settings, privacy settings for IE, Opera pop-ups, Pop-Up Blocker in Safari
[7] דיוג(Phising) - ויקיפדיה
[8] SmartScreen Application Reputation
[9] הערה: תוכנות Anti-Malware אינן מחליפות את תוכנת האנטי-וירוס אלא משמשות כמוצר הגנה משלים.
[10] מחשוב ענן – ויקיפדיה
[11] לדוגמה, רשימת חברות המעניקות שרותי ענן חינם about.com – 33 Free Cloud Storage Services
[12] מדריך לעבודה עם OneDrive

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

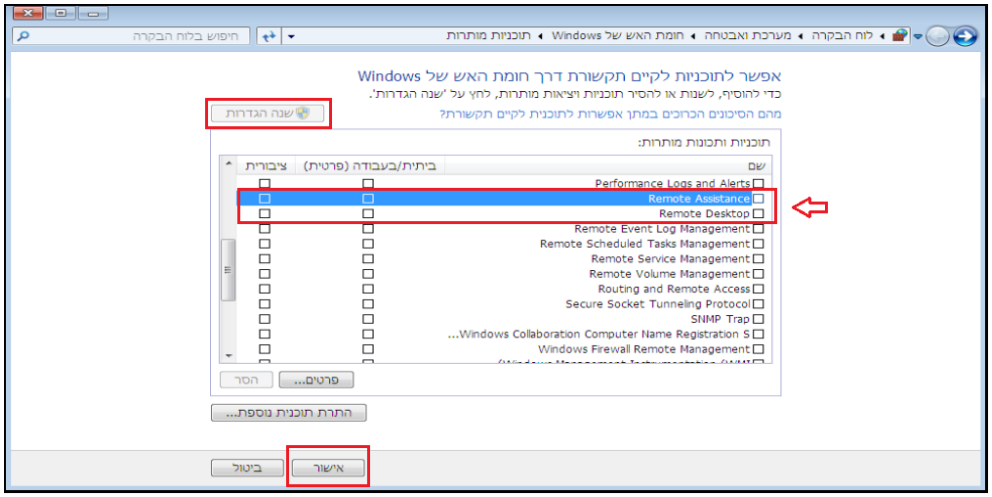
להגדרת ה-UAC של מערכת ההפעלה Windows 7 בחר: לוח בקרה > מערכות ואבטחה > מרכז פעילות > תחת מרכז הפעלות לחץ על "שנה הגדרות של בקרת חשבון משתמש", בחלון שיפתח העלה את המחוג כלפי מעלה לכיוון "הודע תמיד" ולחץ אישור (איור 1).



איור 1. WIN7 UAC

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

להגדרת ה-Firewall הפנימי של מערכת ההפעלה Windows 7 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 2).



איור 2. WIN7 FW

ניתן לשקול בהתאמה לאופי הארגון מספר צעדים:

10. בדיקה כי מערכות ה- Mail Relay מעודכנות באופן תדיר בקובץ החתימות האחרון של יצרן התוכנה.

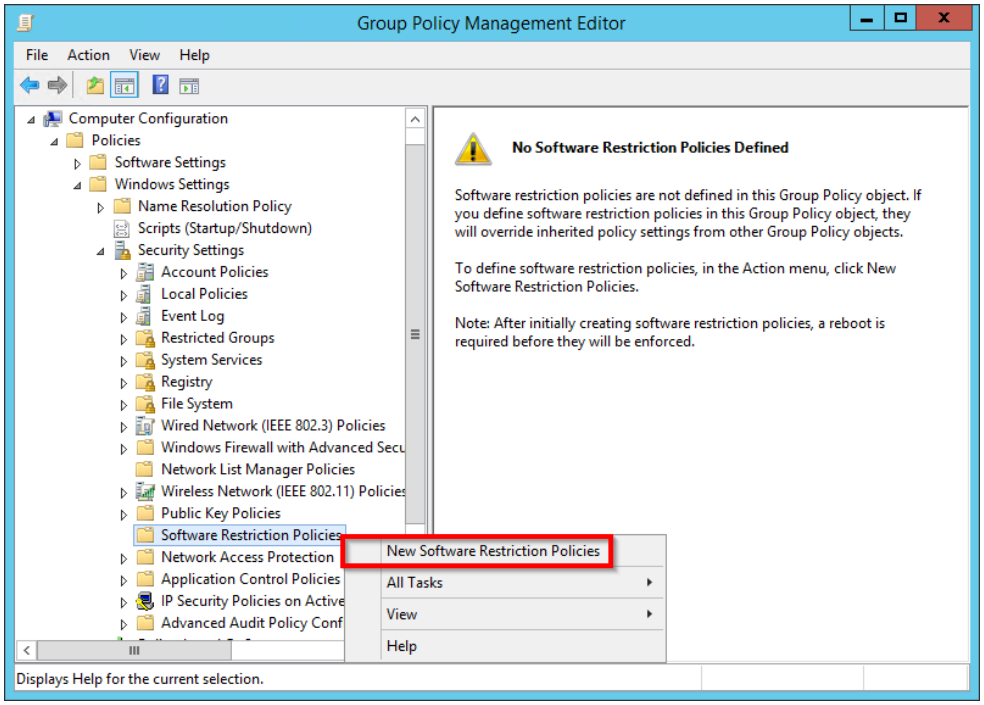
11. לחסום את תעבורת קבצים דחוסים (ZIP/RAR) המכילים קבצי הרצה.

12. הפעלת בקרות להקטנת היכולת לפגיעת סייבר בארגון, לדוגמה באמצעות הפעלת EMET - כלי מובנה חינמי של Microsoft. לפירוט על כלי בקרה זה ובקרות מומלצות נוספות ראו "המלצות להפחתת חדירות סייבר לארגונים - גרסה מלאה גרסה 1.0 יוני 2015" באתר ה-CERT הלאומי.

13. למנוע הפעלת קבצי הרצה במספר ספריות כמו TMP, Download וכדומה על ידי הגדרה של Software Restriction Policy – SRP ב- GPO, באופן הבא:

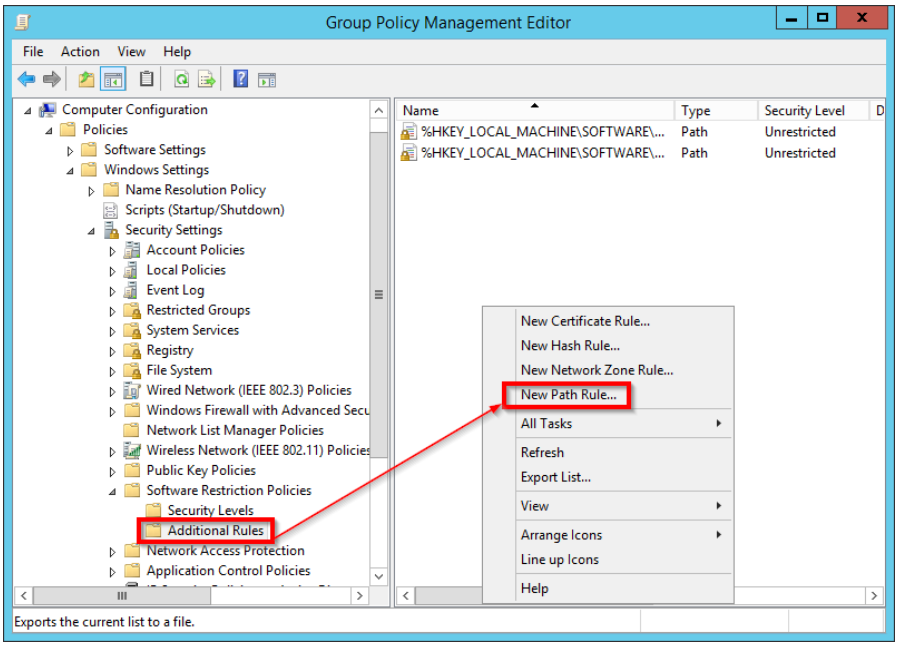
- הפעל את ה- GPO מה- Active Directory ובחר:
- Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies > Additional Rules >

לחיצה על מקש ימני בעכבר ובחירה ב- New Software Restriction Policies(איור 3)



איור 3. New Software Restriction Policies

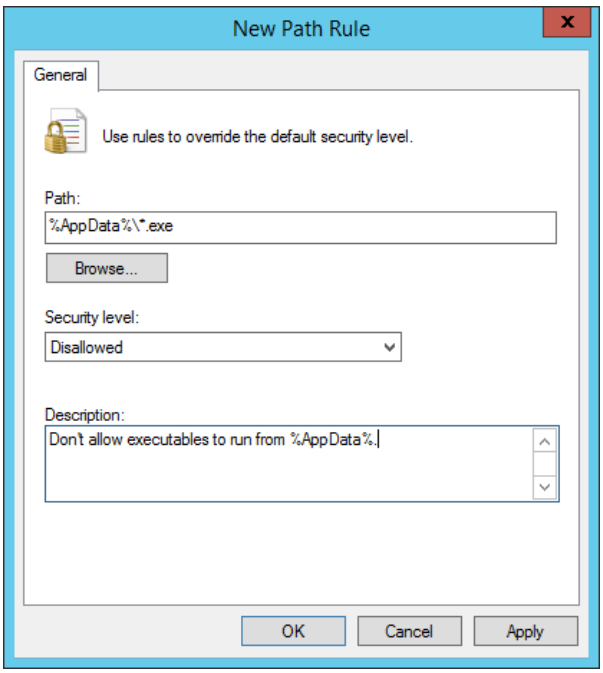
- לחיצה על Additional Rules ואז לחיצה ימנית על New Path Rule (איור 4):



איור 4. New Path Rule

- החלון שיפתח הכנס את הפרטים הבאים לצורך חסימה של הרצת קבצי exe מתיקיית %appdata%(איור 5):

- **Path:** %AppData%*.exe
- **Security Level:** Disallowed
- **Description:** Don't allow executables to run from %AppData%.



איור 5. חסימת הרצת קבצי exe מתיקיית %appdata%

- יש לבצע את הפעולה עבור שאר התיקיות:

חסימה של הרצת קבצי exe מתיקיית :%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 executables to run from %AppData%.

חסימה של הרצת קבצי exe מתתי-תיקיות של %AppData%:

- **Path:** %AppData%**.exe
- **Security Level:** Disallowed
- **Description:** Don't allow executables to run from immediate subfolders of %AppData%.

חסימה של הרצת קבצי exe מתתי-תיקיות של %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 executables to run from immediate subfolders of %AppData%.

חסימה של הרצת קבצי exe הרצים אוטומטית בעת הפעלת WinRAR:

- **Path if using Windows XP:** %UserProfile%Local SettingsTempRar**.exe
- **Path if using Windows Vista/7/8:** %LocalAppData%TempRar**.exe
- **Security Level:** Disallowed
- **Description:** Block executables run from archive attachments opened with WinRAR.

חסימה של הרצת קבצי exe הרצים אוטומטית בעת הפעלת 7zip:

- **Path if using Windows XP:** %UserProfile%Local SettingsTemp7z**.exe
- **Path if using Windows Vista/7/8:** %LocalAppData%Temp7z**.exe
- **Security Level:** Disallowed
- **Description:** Block executables run from archive attachments opened with 7zip.

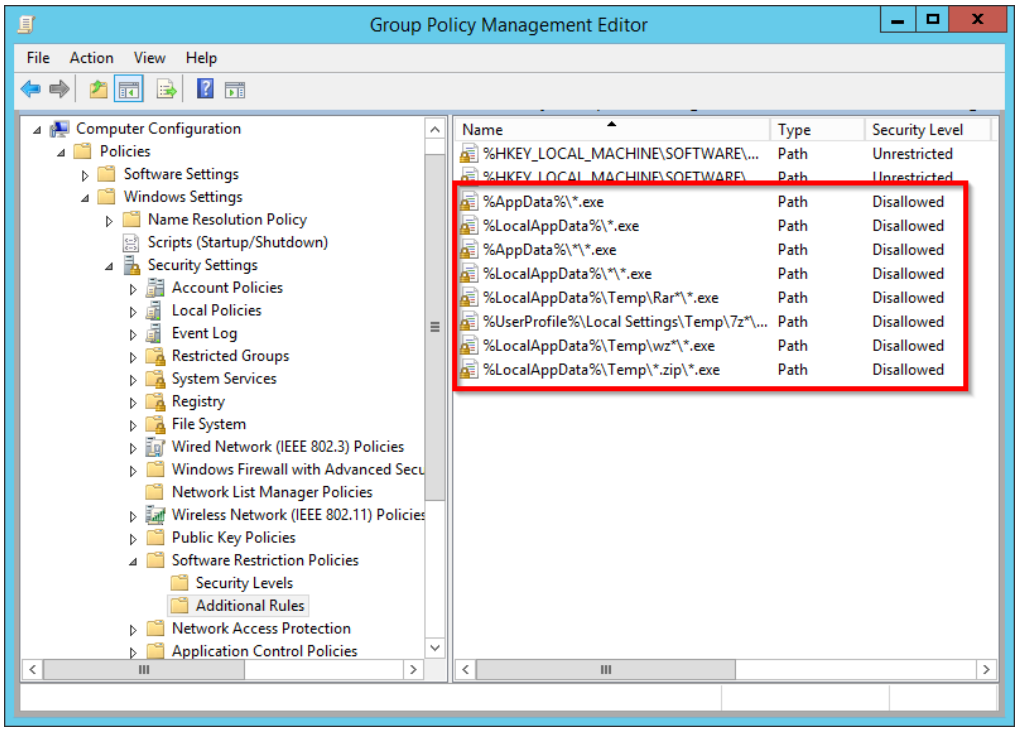
חסימה של הרצת קבצי exe הרצים אוטומטית בעת הפעלת WinZip:

- **Path if using Windows XP:** %UserProfile%Local SettingsTempwz**.exe
- **Path if using Windows Vista/7/8**: %LocalAppData%Tempwz**.exe
- **Security Level:** Disallowed
- **Description:** Block executables run from archive attachments opened with WinZip.

חסימה של הרצת קבצי exe הרצים אוטומטית בעת הפעלת תוכנת Zip המובנת ב-Windows:

- **Path if using Windows XP:** %UserProfile%Local SettingsTemp*.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.

בסיום, החלון צריך להראות כך (איור 6):

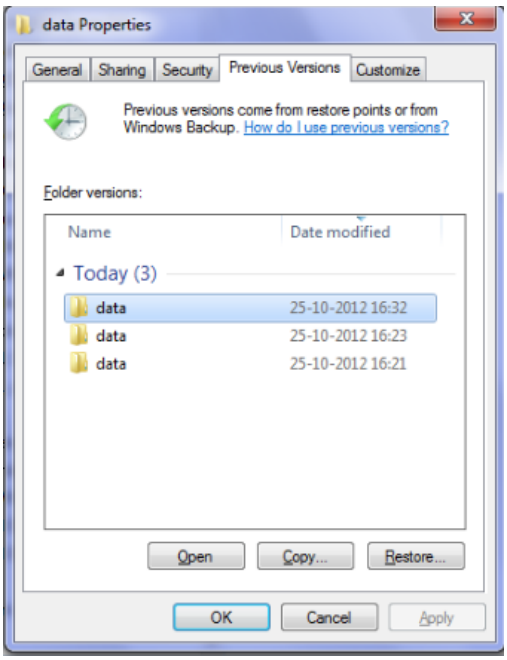


איור 6. לאחר החלת ההגדרות

<u>פעולות אפשריות במידה ועולה חשש לפגיעה בנוזקת כופר או שהוצגה בקשת כופר ברשת הארגונית</u>

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

1. אין 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 את קבצי הלוג של Firewall, IPS, AD, Local System logs
5. לשמור קבצי pcap 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.
7. שחזור גרסאות קודמות של קבצים במחשב, אם כי כבר נצפו סוגים שונים של נוזקות כופר אשר מחפשות ומוחקות את הגרסאות הקודמות, הקשחת ה-UAC עשויה למנוע מהפוגען את יכולת המחיקה.
על מנת לשחזר את הגרסאות הקודמות של הקבצים יש ללחוץ לחיצה ימנית על התיקייה או הקובץ לשחזור ולבחור מאפיינים (Properties) בחלון שיפתח יש לעבור ללשונית גרסאות קודמות (Previous Versions) ולהעתיק את הגרסא הקודמת של הקובץ המבוקש (איור 7).



איור 7. גרסאות קודמות

אינדיקטורים (IOC)

(Indicators Of Compromise) - מאפיינים שנצפו ברשת או במערכת ההפעלה שעשויים להעיד על חדירה או פגיעה במערכות מחשב.

להלן החתימות הידועות ושרתי הפיקוד והשליטה (C&C) שנצפו בתקיפות עבר :

(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)

מיקום קבצי ההרצה של הנוזקה :

- %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>

לנוזקות כופר ישנן גרסאות שונות אשר פועלות בדרכים שונות. על כן, יתכן והכלים המפורסמים בציבור לא יסייעו לפענח בהצלחה את קבצים המוצפנים ולהציל את המידע. טרם ביצוע כל פעולה או ניסיון תיקון באמצעות כלי כלשהו המתפרסם בציבור, יש לנקוט במשנה זהירות, להבין היטב את ההשלכות האפשריות ולדעת כי לא תמיד ניתן יהיה לפענח את ההצפנה ולשחזר את הקבצים.

<u>קישורים ומידע נוסף</u>:

- 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

לכל מידע נוסף ניתן לפנות אלינו.

בברכה,

CERT-IL

טל: 03-7450801

team@cert.gov.il