TLP: White

04 ינואר 2016
כ״ג טבת תשע״ו
סימוכין: ל-ס-165

התרעה על אודות פוגען כופר חדש - CryptoJoker

הודעה

תיאור

בעת האחרונה אנו עדים להמצאותו של פוגען כופר חדש בשם – CryptoJoker. בדומה לפוגענים אותם אנו מכירים מהעבר עושה שימוש בהצפנה מסוג AES-256 על מנת להצפין את קבצי המשתמש. נכון להיום, פוגען זה אינו נפוץ במיוחד אך ייתכן וכי תפוצתו תתרחב בעתיד.

הפוגען הינו קובץ PDF, עובדה זו מעלה את החשד כי הפצתו תעשה באמצעות מתקפות דיוג על מנת להגיע למטרות רבות ככל הניתן. בעת פתיחת הפוגען קבצים נוספים מורדים לתיקיית %Temp% וכן קובץ יחיד לתיקיית %AppData%. קבצים אלו מבצעים פעולות נוספות אשר מהוות חלק מתהליך ההדבקה של המחשב הנתקף (כגון: תקשורת מול שלט השו״ב, סגירת יישומים ועוד).

כמו בפוגענים רבים מסוג זה הפוגען יחפש קבצים (הן מקומית והן בכונני רשת) בעלי סיומות קבועות מראש אשר שמורים על המחשב הנתקף, יצפינם ויוסיף להם את הסיומת crjoker. במהלך ההצפנה נאספים נתונים מזהים על המחשב הנתקף אשר נשלחים לשרת השו״ב.

סיומות אשר תוצפנה:

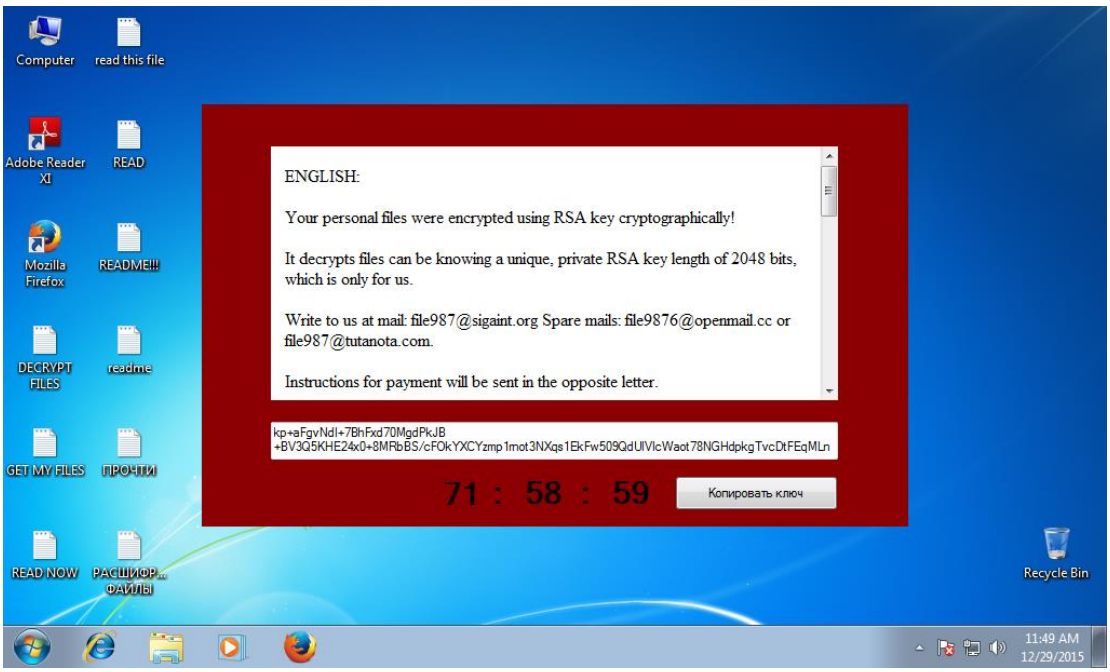
```
.txt, , .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .png, .csv, .sql, .mdb, .sln, .php, .asp, .aspx, .html, .xml, .psd, .java, .jpeg, .pptm, .pptx, .xlsb, .xlsm, .db, .docm, .sql, .pdf
```

על מנת למזער את יכולת המשתמש לשחזר את המידע שהוצפן ממחשבו יוצר הפוגען קובץ batch בספריית %Temp% בשם new.bat. קובץ זה מכיל שורה של פקודות שתפקידן למחוק את ה- Shadow Volume Copies אשר שמורים במחשב הנתקף וכן לבטל את יכולת התיקון האוטומטי של חלונות (Automatic Startup Repair)

הפקודות אשר מבוצעות באמצעות הקובץ:

```
vssadmin.exe Delete Shadows /All /Quiet
bcdedit.exe /set {default} recoveryenabled No
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
vssadmin.exe delete shadows /all /quiet
```

בסיום פעולתו יציג הקורבן את הודעת הכופר בעברית ורוסית.



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)

IP Addresses:

1. 109.237.132.12
2. 213.25.128.10
3. 185.83.208.188
4. 211.214.161.186
5. 70.12.247.47

Domains:

1. server6.thcservers.com
2. daapv.de
3. sayan-sanat.ir
4. pcblueberry.kr
5. tkopd.leszno.pl

Registry. :

1. HKCU\Software\Microsoft\Windows\CurrentVersion\Run\winpnp %Temp%\winpnp.exe
2. HKCU\Software\Microsoft\Windows\CurrentVersion\Run\drvpci %Temp%\drvpci.exe
3. HKCU\Software\Microsoft\Windows\CurrentVersion\Run\windefrag
   %Temp%\windefrag.exe

MD5:

1. 448f787a6e2a0e1907f1abd67f5b85b4
2. bca6c1fa9b9a8bf60eecbd91e08d1323

SHA-1 :

1. 4c17b97a3e20b5f247536d9c8be6cd63e8e1806b
2. 711752953ee347e6797e4b8d835e26b0d32331be

:SHA-256

1. ba4e7b8df8d78a961b30e890c8721fe78c730c0f2c2a85c858369cd3a55f0f13
2. 8bd8901cf7ef997321344a48bd6a754767b01e346e14eae965ba139443353b3

Malicious Emails Addresses:

1. file987@sigaint.org
2. file9876@openmail.cc
3. file987@tutanota.com

Files & Folders:

1. %Temp%\crjoker.html
2. %Temp%\drvpci.exe
3. %Temp%\GetYouFiles.txt
4. %Temp%\imgdesktop.exe
5. %Temp%\new.bat
6. %Temp%\README!!!.txt
7. %Temp%\sdajfhdfkj
8. %Temp%\windefrag.exe
9. %Temp%\windrv.exe
10. %Temp%\winpnp.exe
11. %AppData%\dbddbccdf.exe
12. %AppData%\README!!!.txt22

<u>קישורים ומידע נוסף:</u>

1. https://www.virustotal.com/en/file/ba4e7b8df8d78a961b30e890c8721fe78c730c0f2c2a85c858369cd3a55f0f13/analysis/1451460454/

2. http://www.bleepingcomputer.com/news/security/the-cryptojoker-ransomware-is-nothing-to-laugh-about/

3. https://www.hybrid-analysis.com/sample/ba4e7b8df8d78a961b30e890c8721fe78c730c0f2c2a85c858369cd3a55f0f13?environmentId=1

במידה שבבדיקתכם התגלה ממצא כלשהו נבקש לקבל היזון חוזר.
לכל מידע נוסף ניתן לפנות אל ה- CERT הלאומי באמצעות פרטי ההתקשרות המפורטים בסוף המסמך.

הערה חשובה : שיתוף מידע עם ה- CERT-IL איננו מחליף את חובת הדיווח לגוף מנחה כל שהוא, במידה והתגלה צורך כזה.

המלצות להפחתת סיכונים

המרכז להתמודדות עם איומי סייבר CERT-IL רוצה להזכיר למשתמשים ולמנהלים מספר דגשים ממומלצים כדי לחזק את מצב האבטחה שלהם במערכות הארגון:

- לשמור על מנועי מערכות האנטי-וירוס והחתימות מעודכנות תמיד.
- להגביל את יכולתם של המשתמשים (הרשאות) להתקין ולהפעיל יישומי תוכנות לא רצויים.
- לאכוף מדיניות סיסמא חזקה וליישם שינויי סיסמא תקופתיים.
- לנהוג במשנה זהירות בעת פתיחת קבצים מצורפים לדואר אלקטרוני, גם אם הקובץ המצורף היה צפוי והשולח נראה מוכר.
- לשמור על מערכות ההפעלה מעודכנות וליישם מידית כל טלאי אבטחה שמופץ.
- להסיר תוכנות ישנות ולא נחוצות, ולדאוג לעדכון גרסאות של האחרות ויישום טלאי האבטחה.
- להפעיל חומת אש אישית בתחנות העבודה.
- לנטרל שירותים מיותרים בתחנות עבודה ובשרתים.
- לסרוק ולהסיר קבצים חשודים המצורפים לדואר אלקטרוני; להבטיח כי הקובץ המצורף שנסרק הוא "סוג הקובץ האמיתי" (כלומר הסיומת מתאימה לכותרת קובץ) ולחסום קבצים עם סיומות הרצה.
- לבצע ניטור להרגלי הגלישה באינטרנט של משתמשים; להגביל את הגישה לאתרים עם תוכן שלילי.
- לנהוג במשנה זהירות בעת השימוש באמצעי אחסון נשלפים (USB, כוננים חיצוניים, תקליטורים, וכו').
- לסרוק כל תוכנה שמורדת מהאינטרנט לפני התקנתה.
- לשמור על מודעות מצבית של האיומים האחרונים, וליישם רשימות בקרת גישה מתאימות.

לרשימת בקרות מומלצות להפחתת חדירות סייבר לארגונים ראו באתר ה- CERT בקישורים הבאים:

https://cert.gov.il/Resources/best_practices/SiteAssets/Cert-Il%20Best%20Practices%20short%20booklet%20.pdf

https://cert.gov.il/Resources/best_practices/SiteAssets/CERT-IL%20Best%20Practices%20Full%20Booklet.pdf

שאלות ותשובות

האם אני יכול להפיץ מסמך זה לאנשים אחרים? מסמך זה מופץ כ- TLP ירוק. מקבלי מידע ב- TLP ירוק יכולים לשתף את המידע עם עמיתים, שותפים, ארגונים במגזר או בקהילה שלהם, אך לא דרך ערוצים נגישים לציבור. לגבי פניות הפצה ספציפיות אנא צור קשר עם עמנו קשר.

האם אני יכול לערוך את המסמך הזה? מסמך זה לא ניתן לעריכה בכל דרך שהיא על ידי שום גורם מלבד CERT-IL. כל ההערות או השאלות הנוגעות למסמך יש להפנות למרכז להתמודדות עם איומי סייבר בטלפון 03-7450801 או באמצעות הדואר האלקטרוני בכתובת team@cert.gov.il.

האם אני יכול להעביר לחקירה תוכנות זדוניות ל- CERT-IL? CERT-IL מעודד אותך לדווח על כל פעילות חשודה, כולל תקריות אבטחה מקוונות, קוד זדוני אפשרי, נקודות תורפה והונאות הקשורות לגניבה זהות. ניתן לדווח בטלפון 03-7450801, באמצעות הדואר האלקטרוני בכתובת team@cert.gov.il או באמצעות דף צור קשר באתר https://cert.gov.il/ContactUs/Pages/ContactUs.aspx

פרטי התקשרות

טל: 03-7450801
דוא"ל: team@cert.gov.il
אתר: www.cert.gov.il
PGP Fingerprint: 9D4C24D29A306BD2AFEA4437E2448206F7C085AF