25 בספטמבר 2019
כ"ה באלול תשע"ט
סימוכין: ב-ס-996

קמפיין דיוג המתחזה לרשות האכיפה והגבייה

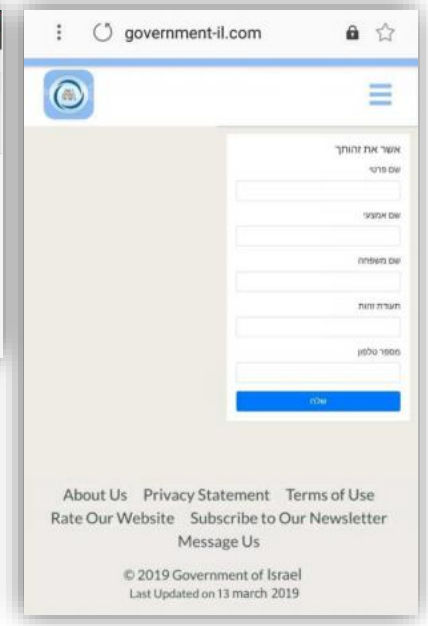
תקציר

1. החל מסוף השבוע שעבר החלו להתקבל ב-CERT הלאומי דיווחים אודות קמפיין דיוג אשר במסגרתו נשלחו הודעות דוא"ל לנמענים רבים, לכאורה מטעם רשות האכיפה והגבייה.
2. מחקירה של ה-CERT הלאומי, של גורמי אכיפה ושל חברות אבטחת מידע, עולה כי הודעות הדוא"ל נושאות את השם "הוצאה לפועל- מכתב תביעה", ומכילות קובץ זדוני המוריד נוזקת כופרה (Ransomware).
3. מחקירה של ה-CERT הלאומי עולה כי מדובר בכופרת Buran אשר נמכרת באינטרנט כשירות (RaaS).
4. כמו כן, נמצא כי התוקפים השתמשו בשירות דוא"ל זמני אשר אפשר להם לתקשר עם הקורבנות זמן קצר לאחר שליחת דוא"ל הדיוג.
5. עד כה ידוע על מספר בודד של אזרחים ועל חברה אחת שפתחו את הצרופה ונדבקו בכופרה.
6. מטרת מסמך זה היא התרעה למשק אודות האירוע, שיתוף מזהים ומתן המלצות.

רקע

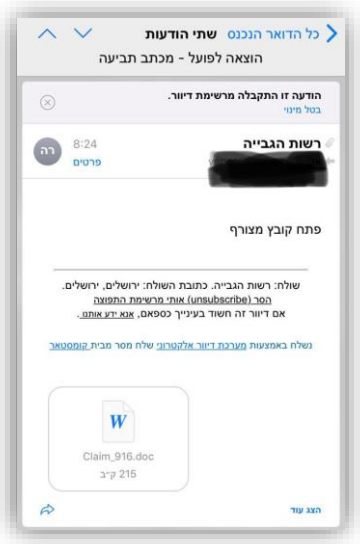
1. התחזות לארגונים ממשלתיים היא שיטה מוכרת ונפוצה לביצוע מתקפות, שכן היא מוסיפה נופך של אמינות ודחיפות לבקשת התוקפים, וכך מניעה את הקורבן לביצוע פעולות.

2. בנוסף לקמפיין דיוג זה אשר כלל התחזות לרשות האכיפה והגבייה, נחשפו השנה מתווי תקיפה דומים נוספים. דוגמאות לכך הן קמפיין דיוג שנחשף השבוע שבמסגרתו נשלחו הודעות דוא"ל המתחזות למשרד המיסים האוסטרלי (ATO) ואשר הובילו לאתר דיוג הגונב פרטי דוא"ל של משתמשים (להרחבה), וכן קמפיין דיוג נוסף שארע השנה שבמסגרתו נשלחו הודעות דוא"ל המתחזות לרשות המיסים הישראלית במטרה לאסוף פרטים אישיים של משתמשים, כגון: שם מלא, מספר זהות, מספר טלפון, תמונה אישית, תמונה של תעודה מזהה ופרטי חשבון בנק (להרחבה).



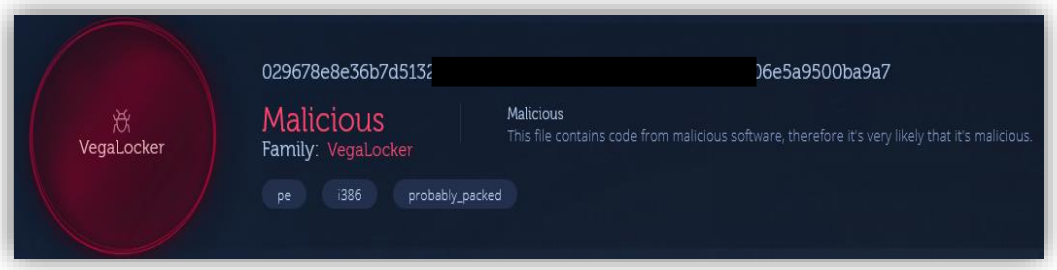
פרטי אירוע

1. ב-12 לספטמבר התקבלה ב-CERT הלאומי אינדיקציה ראשונית לקיומו של קמפיין דיוג, אשר במסגרתו מופצות הודעות דוא"ל המתחזות לרשות האכיפה והגבייה.
2. להודעות הדוא"ל צורף קובץ DOC בשם "Claim_916.doc".
3. להלן צילום מסך של הודעת הדיוג:



4. מחקירת ה-CERT הלאומי עלו הממצאים הבאים:

- להודעות הדוא"ל צורף קובץ DOC המכיל בתוכו פקודות מאקרו, אשר בעת הרצת הקובץ מורידות נוזקה מסוג כופרה למחשב.
- מהשוואה של קטעי קוד (Code Similarity) עולה כי מדובר בנוזקה ממשפחת הכופרות Vegalocker, אשר מכונה "Buran". בין היתר, משפחה זו כוללת את הווריאנטים: "Vega", "Ghost" ו-"Jamper".

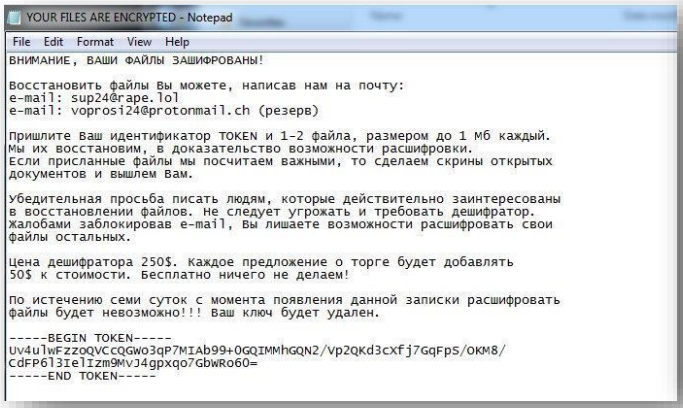


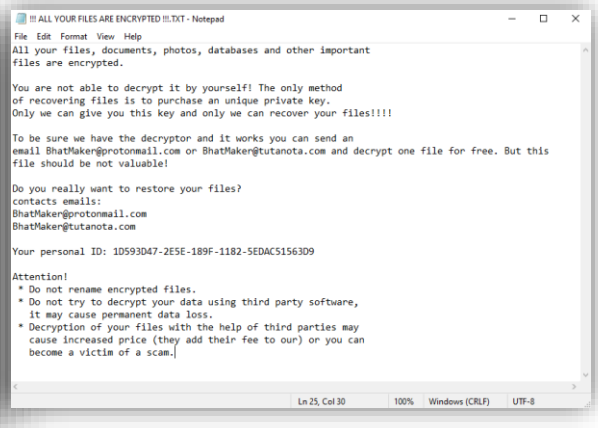
- כמו כן, מבדיקה עולה כי נוזקות ממשפחת VegaLocker נמכרות על-ידי קבוצת פשיעת סייבר רוסית כשירות (RaaS), תוך קיום משא ומתן עם הרוכשים בנוגע לתנאי המכירה וההפעלה. ככל הנראה, רוכשי השירות מתחייבים להעביר לקבוצה אחוזים מסוימים, הנעים בין 25% ל-40%, מסך תשלומי הכופר שיתקבלו.
- יש לציין כי חברי הקבוצה הצהירו לא פעם כי הנוזקה לא תפעל במדינה החברה בחבר המדינות (CIS). אף על פי כן, מחקירת קוד הנוזקה עולה כי היא הוגדרה שלא לפעול רק ברוסיה, בבלארוס, בקזחסטן ובאוקראינה.
- להלן צילום פרסום של מכירת השירות:

We are waiting for new adverts! Why us, and not other affiliate programs? * We have never been decrypted, avers repeatedly perf ormed a detailed analysis and analysis of software, a free decoder was not and will not be released; * We use our own algorithm f or processing large files, not the first kilobytes of data are encrypted (many archives can be partially restored after such encryptio n), not the entire file (a very resource-intensive **operation** , it takes a lot of time), but randomly selected fragments, this gives an ad vantage in speed and reliability; * Our software runs on the entire line of Windows, starting from Windows XP; * In many matters, we meet adverts, provide round-the-clock support, advise everyone in detail and tactfully; * We do not sell builds, key generation and rebuilds are free; * With us you are guaranteed to earn;) Reminder: * We do not work in the **CIS** (a locale detection is installed + the language of the system); * We do not work with technically illiterate and far from the topic; * We may refuse to issue a build without explanation; Join the affiliate program: **buransupport@thesecure.biz buransupport@exploit.im**

- אחת התכונות הייחודיות של הוריאנט "Buran" היא שבמהלך הרצת הכופרה במחשב, סיומת הקבצים משתנה על-פי ID ייחודי לכל משתמש ולא על פי סיומת קבועה כמו בכופרות אחרות, דבר המקשה על זיהוי של מערכות ההגנה השונות.
- הנוזקה מותאמת לפעול במערכות הפעלה Windows בגרסאות XP והלאה, כולל Windows Server.

- להלן דוגמאות לצילומי מסך של דרישות תשלום הכופרה כפי שהופיעו במחשבי הקורבנות:





5. מחקירת האירוע עולה כי ככל הנראה התוקפים שכרו שירות של חברת דיוור באמצעות כרטיס אשראי גנוב, וכי הדוא"ל הזדוני נשלח לרשימת התפוצה של אותה החברה אשר כללה 600,000 כתובות דוא"ל. מתוך אלו, הדוא"ל הזדוני נשלח ל-200,000 נמענים, וידוע כי 80,000 פתחו אותו.
6. כמו כן, נמצא כי התוקפים השתמשו בשירות דוא"ל זמני שאפשר להם לתקשר עם הקורבנות זמן קצר לאחר שליחת דוא"ל הדיוג, במטרה להדריכם כיצד לפתוח את הצרופה ולאפשר הרצה של פקודות המאקרו.

דרכי התמודדות

1. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם במערכות הארגוניות.
2. במידה וקיבלתם דוא"ל העונה לתיאור המופיע בהתרעה זו, יש למחוק אותו באופן מידי ובשום אופן לא להוריד את הקובץ המצורף אליו.
3. במידה וקיבלתם שיחה טלפונית מגורם המנסה להניע אתכם לביצוע פעולות במחשב, נתקו את השיחה והתקשרו לגוף הרלוונטי לבירור הנושא.

4. שימו לב כי דוא"ל או קישורים המגיעים מגורם ממשלתי לעולם יהיו תחת שם המתחם GOV.IL. עם זאת, אין מניעה לנסיונות התחזות גם לשם מתחם זה, ולכן כל בקשה לפרטים אישיים או תשלום יש לוודא טלפונית או באתר הרשמי של הגוף הפונה.
5. מומלץ להפעיל שיקול דעת בפתיחת הודעות דוא"ל, הפעלת צרופות או גישה לקישורים שהגיעו משולחים שאינם מוכרים, או אף משולחים מוכרים אך באופן בלתי צפוי.
6. חפשו סימנים חשודים:
   - הסתכלו על פרטי השולח בדקדקנות, ייתכן ויש זיוף בשם השולח כך שיראה לגיטימי.
   - היו מודעים לניסיונות להאיץ בכם לביצוע מהיר של הנחיית השולח באמצעות איום בסנקציה או אולטימטום לביצוע.
7. לא מכירים את השולח? אל תפתחו את הדוא"ל אם אין הכרח לכך, והימנעו מהפעלת קישורים או פתיחת צרופות (Attachments).
8. מומלץ שלא לאפשר הרצה אוטומטית של פקודות מאקרו ביישומי Office שכן נעשה בהם שימוש במתקפות רבות להורדת נוזקות. להרחבה ראו פרסום של מערך הסייבר הלאומי אודות אבטחת פקודות מאקרו (Macros) ביישומי Office.
9. ראו פרסום של מערך הסייבר הלאומי אודות התגוננות מדואר אלקטרוני זדוני.
10. ראו פרסום של מערך הסייבר הלאומי אודות התמודדות עם נוזקה מסוג כופרה.

שיתוף מידע עם הCERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כלשהו, במידה שהתגלה צורך בזה

בברכה,
CERT-IL