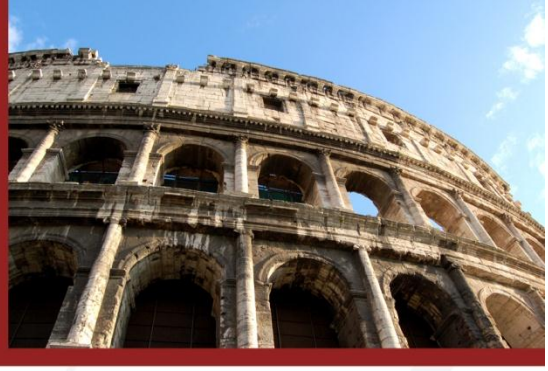


27/11/2012

אשנב לחדשות | אירועים | פוגענים בסייבר

"Narilam"

1. רקע

בימים האחרונים הפיצה חברת "סימנטק" מאמר המפרסם בקצרה את הימצאותו של פוגען חדש שזכה לכינוי "W32.Narilam". על פי הפרסום, עיקר הנזק אשר נגרם עד כה על ידי הפוגען נוצר בתחומי איראן בחברות מסחריות.

מכיוון שנראה היה כי מדובר במתקפה השייכת למתקפות הממוקדות והמתוחכמות, החלטנו לבחון מקרוב את הפוגען במעבדות הסייבר שבחברת "קומסק" לטובת ניתוח יכולות הפוגען והפקת לקחים למטרות שיפור מענה ההגנה הקיים בקרב לקוחותינו.

הממצאים שהועלו כתוצאה מהמחקר מובאים במסמך להלן.

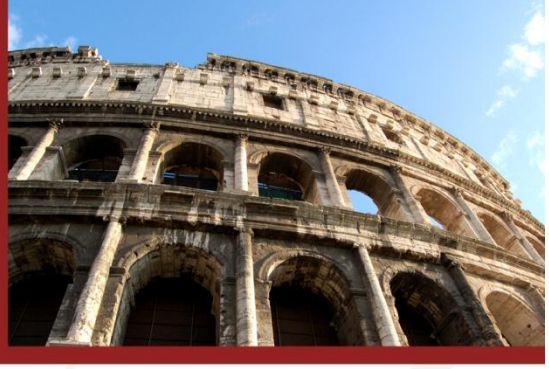
2. פרטים אודות הפוגען

מטרת הפוגען הינה לחבל במסדי נתונים פיננסיים, בפרט בנתונים בעלי מאפיינים ממדינת אירן (על פי שמות השדות אליו ניגש הפוגען). מלבד פעילות זו, מוטמע בקובץ ההרצה מנגנוני הסוואה, התקנה לזמן ממושך וטכניקות העתקה-עצמית לצורך התפשטות.

שיטת ההתפשטות של הפוגען הנה באמצעות הדבקה של כונני רשת או התקני USB (אם כי ללא שימוש ב- Exploits ידועים כגון LNK או Autorun). טכניקת ההדבקה הראשונית אינה ידועה כרגע.

הפוגען הנו בדמות של קובץ יחיד בעל מסווה תמים למראה המנסה להסוות את עצמו כתיקיית קבצים, אף הצלמית של קובץ ההרצה נראה כצלמית תיקייה לגיטימית של מערכת ההפעלה Windows. זאת ועוד, בסוף תהליך הרצת הקובץ נפתחת תיקייה שרירותית במחשב המותקף על מנת לשדר פעולה שגרתית של פתיחת תיקיית קבצים.

1. מראה צלמית קובץ ההרצה של הפוגען, מסווה כתיקיית קבצים



בהגדרות ברירות-מחדל של מערכת הפעלה Windows, משתמש אינו מבחין בסיומות קבצים ולכן הקובץ מקבל לגיטימיות יתרה במראהו התמים חסר הסיומת. נראה כי הגורם שיצר את הפוגען שם דגש על צורת התפשטות בהתבסס טכניקות הלקוחות מארסנל ההנדסה החברתית.

בהרצת הקובץ, מתבצעות כמה פעולות ראשוניות:

1. בדיקת הגדרות השפה במכונה.
2. בדיקת משתנים סביבתיים.
3. אבחון מיקום הקובץ.

בהמשך, ההרצה מבצעת מספר מהלכים זדוניים על מנת לשמור על אפשרות ריצה לעתיד, בעת הפעלה מחדש של המחשב הנגוע:

1. העתקה של קובץ ההרצה כמות שהוא אל המיקום c:\windows\system32\lssas.exe, הגדרת הקובץ החדש כקובץ מוסתר, הגדרת תאריך עדכון הקובץ אל 22/10/10.
2. יצירת קובץ חדש תחת תיקיית System32 בשם fcB32Df.ocx, כתיבת תאריך ההרצה אל תוכן הקובץ הנוצר.
3. הוספה של הפעלה אוטומאטית ברמת Registry אל HKLM\Software\Microsoft\Windows\CurrentVersion\Run – בשם מפתח LssasShellExt.
4. במקרים מסוימים, הפוגען ינסה להעתיק את עצמו גם אל תיקיית ההפעלה – Stratup.

מאפייני הקובץ כוללים:

1. עפ"י פרסומים נראה כי ישנן מספר גרסאות לקובץ, הגרסה שברשותנו תואמת לחתימה
   MD5: 0d33edb34fb00754914900faf7814bd6
   SHA1: c789a65f5a2914bf6090169c61e6b29364a21361
2. גודלו הלוגי של הפוגען הינו 1,577,472 בייט. Image מסוג PE32.
3. שפת התכנות שהשתמשו בה לבנייתו הינה Delphi, בעזרת ספריות של המהדר Borland.
4. בפרטי הקובץ נרשם כי החברה היוצרת הנה Microsoft, עם זאת הקובץ **אינו** חתום בחתימה דיגיטאלית.
5. שמו המקורי של הקובץ הינו lssas.exe, בדומה לשם קובץ לגיטימי (lsass.exe) במערכת ההפעלה, בכוונת תחילה על מנת להסתיר את פעולתו ברקע ולשכנע את המשתמש בלגיטימיות שלו.
6. במאפייני הקובץ מזוהה כ-Locale בשפה הפרסית.
7. תאריך העדכון של הקובץ (ניתן לזיוף) - 22 לאוקטובר 2010.
8. קומפל בבורלנד 99', תאריך הקימפול המוטבע (ניתן לזיוף) – 12 ליוני 2010.

3. מטרת הפוגען

כאמור, נראה כי מטרתו הראשית של הפוגען הינה חבלה במסדי נתונים פיננסיים ובפרט איראניים, ניתן לזהות זאת על ידי אבחון הקובץ מקרוב והמידע הנשמר בזיכרון בעת הרצתו. שמות מסדי הנתונים ורשומותיהם מאופיינים בשמות בפרסית בשעתוק לאנגלית. לדוגמה – Hesabjari (חשבון נוכחי) ו-Pasandaz (חסכונות).

```
:005455DF   Set @SanadNo1=Round(@SanadNo1 * (SELECT RAND(@IDLE)),0,0)
:0054561B   Update Asnad Set SanadNo=@SanadNo1,LastNo=@SanadNo1,FirstNo=(
:00545694   set @SanadNo=(select Max(Cast(sellercod As int )) from A_Sellers)
:005456D8   Set @SanadNo=Round(@SanadNo * (SELECT RAND(@IDLE)),0,0)
:00545712   delete from A_Sellers Where Cast(sellercod as int)=@SanadNo
:00545751   set @SanadNo=(select Max(Cast(Tranid As int )) from A_TranSanj)
:00545793   set @SanadNo1=@SanadNo
:005457AC   Set @SanadNo=Round(@SanadNo * (SELECT RAND(@IDLE)),0,0)
:005457E6   set @Raj=(select Max(Raj) from A_TranSanj Where Cast(Tranid as int)=@S
:00545836   Set @Raj=Round(@Raj * (SELECT RAND(@IDLE)),0,0)
```

2. דוגמה לשאילתות הנטענות לזכרון בעת הרצת הקובץ

השאילתות שנמצאו מתארות מחיקה ושיבוש (תלוי מקרה) של נתונים לטבלאות שונות כגון נתוני חשבונות בנק, שמות לקוחות, נתוני הלוואות וחסכנות, אגרות חוב, טבלאות שכר, חופשות וכד'.

לאחר פרסום הפוגען, חברת TarrahSystems האיראנית, אשר מפיקה מערכות לניהול פיננסי באיראן ובשפה הפרסית דיווחה בעמוד הבית שלה על שינוי במערכותיה בעקבות הפוגען.

3תמונת מסך מאתר החברה TarrahSystems המתריעה בפני הפוגען

שמות מוצרי החברה מוטבעים ברמת הקוד הזדוני ולכן ההיתכנות גבוהה כי הפוגען כוון לשימוש כנגד מערכות אלה בפרט, אם כי הדבר לא ניתן כרגע מהמידע הקיים בידנו לאימות חד משמעי.

עד כה, מהבחינה שבצענו, לא נראה כי נעשה שימוש ב-Exploit ידוע או Zero Day בשום שלב. הפוגען מסתמך על הרשאות הגישה של המשתמש אשר פותח את הקובץ (חובה בהפעלה ידנית) ועל טכניקות שונות של הנדסה חברתית.

בנוסף, בניגוד לפוגענים מתקדמים שראינו עד כה, נראה כי הפוגען הזה הנו בעל יכולות בסיסיות בלבד ואינו ניתן לשליטה מרחוק ע"י שרתי C2 (שו"ב) בניגוד למקובל בקרב פוגענים מתקדמים.

4. המלצות ראשוניות להתמודדות

1. אף כי נכון לעכשיו לא נצפה סיכון לתוכנות אחרות המשתמשות בבסיסי נתונים אחרים מלבד זה של חברת TarrahSystems, ראוי לקחת משנה זהירות ולהתגונן בפני הפוגען ולמוחקו.
2. מומלץ לבצע עדכון תוכנת האנטי וירוס על גבי תחנות הקצה. הפוגען כיום מזוהה מרבית חברות האנטי וירוס לרבות Symantec, Kaspersky ו-McAfee. במידת הצורך ניתן לפנות לצוות מעבדות הסייבר שבחברת "קומסק" לטובת בדיקה ממוקדת של מענה ההגנה המוטמע בארגון.
3. בצוע מחקר פורנזי בדיעבד (ברמת שרתים ותחנות קצה) לפי המידע הנמצא במסמך זה יכול לאתר סימנים המעידים על הדבקה נוכחית / הדבקת עבר.

5. סיכום

מהמידע אשר הגיע לידנו וכתוצאה מניתוח הפוגען עולה כי הפוגען כוון במיוחד למטרות איראניות באוריינטציה עסקית, אין התרשמות כי בוצעו נסיונות מיוחדים להסוואת פעילות התוכנה למעט הטמעתה במערכת ההפעלה וניצול חולשות בסיסיות ברמת הנדסה חברתית על מנת לאפשר לקובץ לרוץ בבטחה, כמו כן – האפשרויות השונות של הפוגען להתפשטות בסיסית ברשת הקרובה אליו.

לעומת פוגענים שכוונו כנגד איראן בשנים האחרונות, הן במידת המורכבות והן מבחינת מטרות הפוגען – מדובר בפוגען פרימיטיבי יותר אשר אינו יודע להתאים את עצמו לסביבתו או בעל אפשרויות שו"ב מרוחק. לפיכך, במיוחד לאור המורכבות הנמוכה של הפוגען, ניתן להניח כי גורם האיום יכול להיות גורם עסקי מתחרה או גורם לאומני בעל רמת תחכום נמוכה אם כי בסבירות נמוכה יותר.

חשוב לציין שאין להסיק מיכולותיו הבסיסיות של הפוגען על רמת הנזק אותו הוא מייצר אשר עשויה להיות משמעותית ליעד הנתקף בהיעדר אמצעי הגנה והתמודדות עם פוגענים "אלימים" מסוג זה.

לסיכום, פוגען זה מצטרף לסדרה ארוכה של מתקפות סייבר ייעודיות בשנים האחרונות באזור המזרח התיכון. למרות רמת התחכום הנמוכה נראה גם במקרה זה מדובר בפוגען ייעודי אשר נתפר באופן ייחודי ליעד ומתוך מטרה לייצר נזק למערכות מחשוב רגישות של היעד.