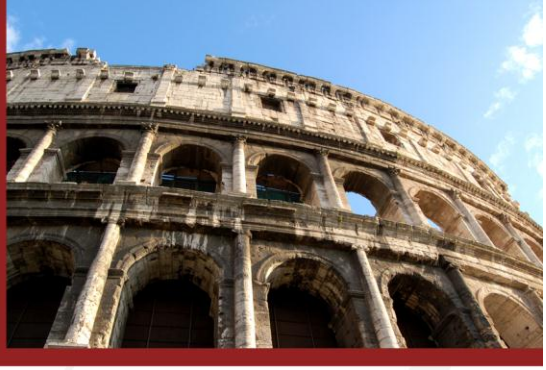


20/12/2012

אשנב לחדשות | אירועים | פוגענים בסייבר

# סקירת פוגענים – Dexter

## 1. רקע

לאחרונה, התגלה פוגען בתפוצה רחבה של מאות יעדים ובמספר רב של מדינות אשר זכה לכינוי Dexter ואשר מתכנניו שמו להם למטרה עמדות "קופה" ממוחשבות (POS / Point-of-Sale). ייעודו של הפוגען הנו האזנה לנתוני כרטיסי אשראי / פסים מגנטים וגניבתם באמצעות שליחתם לשרתי שו"ב מרוחקים.

**Figure 1עמדת POS טיפוסית בעלת מסך מגע (cc-sa-2.0 imtfi@flickr)**

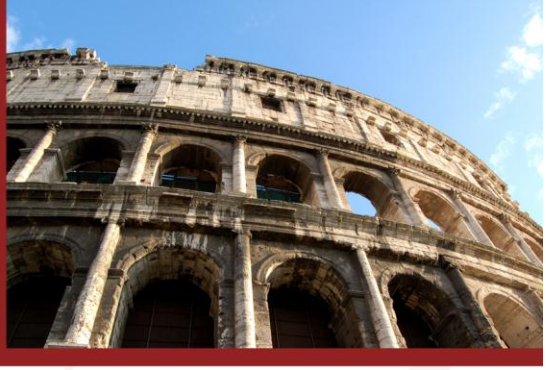
אמנם Dexter אינו נחשב לפוגען הראשון המבצע סוג כזה של גניבת נתוני אשראי אך תפוצתו ויעילותו הפנו אליו זרקורים רבים, מה שהוביל לבחינה מעמיקה של הפוגען במעבדות הסייבר אשר בחברת קומסק. מטרת נייר זה לספק תמונה רחבה אודות גורמי האיום ותסריטי התקיפה לטובת שיפור מענה ההגנה וההערכות בקרב לקוחותינו.

## 2. פרטים אודות הפוגען

משקלו (גודלו) הכולל של הפוגען הנו כ- 50KB כאשר הוא מורכב מקובץ אחד בודד.

**מספר מאפיינים ודגשים אודות תהליך ההדבקה:**

1. לטובת ההדבקה של התחנה יש לבצע הרצה של קובץ ההתקנה (ה-Executable) של הפוגען. טכניקת ההפצה וההפעלה הראשונית אינן ידועה.
2. כרגע לא ידוע על יכולות התפשטות של הפוגען למחשבים אחרים.
3. הפוגען מעתיק את עצמו בשם רנדומאלי לתיקיית %UserProfile% במחשב הנתקף. ההעתקה נעשית ע"י הזרקה של הקוד ל-iexplore.exe וגרימה לתהליך לכתוב את קוד הפוגען לתיקיית %UserProfile%.
4. מיד עם ביצוע ההתקנה הפוגען מוחק את קובץ ההתקנה המקורי.
5. לאחר מכן הפוגען מנסה לשדר לשרתי ה-C2 (שרתי השו"ב של הפוגען).



**שינוי Registry במחשב:**

- HKEY_CURRENT_USER\Software\Resilience Software\Digit = "[מספר מסמל]"
- HKCU\software\ms\windows\currentversion\policies\associates = ".exe;.bat;.reg;.vbs"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\[מספר מסמל] = "%UserProfile%\[תווים אקראיים].exe"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\[מספר מסמל] = "%UserProfile%\[תווים אקראיים].exe"

1. השינוי הראשון נועד ככל הנראה למנוע מצב בו הפוגען מנסה להתקין עצמו מספר פעמים על אותו מחשב, כך הוא מסמן את המחשב הנגוע ובהרצה שנייה מזהה את הKey ולא מבצע את פעולות ההשתלטות העוינות בשנית.
2. השינוי השני נועד כדי לאפשר הרצת קבצי אצווה על גבי המחשב מבלי שהמשתמש יקבל התרעה ממערכת ההפעלה אודות ההרצה.
3. שני השינויים האחרונים מהווים שיטת עליה ומאפשרים את ריצת הפוגען לאחר ביצוע אתחול למחשב.

**קבצים שהפוגען יוצר:**

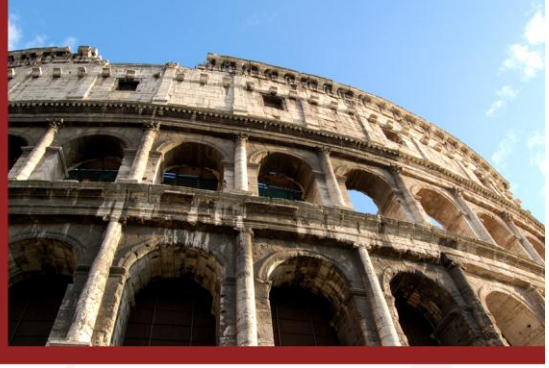
- קובץ ההרצה של הפוגען - %UserProfile%\[תווים אקראיים].exe

**מאפיינים ודגשים אודות קובץ הפוגען:**

1. הקובץ דחוס ומקודד באופן ייחודי (לא נעשה שימוש ב-Packer מוכר) דבר אשר אינו נחשב לסטנדרטי ומוסיף במידה מסוימת למידת התחכום של המתקפה.
2. קוד ההרצה המקורי של הקובץ נפתח בזיכרון בלבד.

**מאפיינים ודגשים אודות תהליך הריצה:**

1. הפוגען מריץ שני תהליכים של Internet Explorer. הפוגען משתמש בתהליך זהה לצורך שידור HTTP בפורט 80. תהליך שכזה שכיח בפוגענים למטרת הסוואת תוכן זדוני שכן משתמש אשר מאזין לתקשורת יתקשה לזהות תקשורת עוינת כאשר היא נוצרת על ידי תוכנה לגיטימית ובאופן שסביר למצוא את שאר התקשורת של התוכנה המזוהה כזהים או דומים מאוד לתשדורת העוינת.
2. אחד מתהליכי ה-Internet Explorer שנוצרו משמש כ-Watchdog – פתיחת Instance חדש של Internet Explorer במידה והקודם ייסגר.
3. הפוגען מסוגל להוציא נתונים מהמחשב עליו הוא מתוקן לרבות:
   א. **מידע מהזיכרון**. מידע זה מתקבל ע"י בחינת הזיכרון של כל התהליכים הרצים. הפוגען מזהה תבניות של כרטיסים מגנטיים – זוהי מטרת-העל של הפוגען.
   ב. Username.
   ג. שם מחשב.
   ד. מערכת הפעלה.
   ה. רשימת תהליכים.



**מאפיינים ודגשים אודות תהליך הדיווח:**

1. הפוגען יוצר קשר עם שרת C2 (שרת שו״ב) לכתובות מרובות הנראות כך:
   fabcaa97871555b68aa095335975e613.com
   67b3dba8bc6778101892eb77249db32e.com
   815ad1c058df1b7ba9c0998e2aa8a7b4.com
   ישנן מספר רב של דגימות שונות במקצת של הפוגען, כך שחלקן מפנות לאתרים אחרים בפורמט זהה. יש אף כמה מהדגימות אשר מכיל כתובות IP קבועות המוטבעות בקוד שלהן כאשר ככל הנראה מדובר בדגימות של גרסה מוקדמת יותר של המתקפה.
2. מרבית הכתובות הינן כתובות דינאמיות אשר עלולות כמובן להשתנות.
3. הפוגען משדר בפורט 80 (פרוטוקול HTTP) ומבצעת POST ל-URI /portal1/gateway.php
4. ה-User Agent המשמש את הפוגען לשידור הוא Mozilla/4.0(compatible; MSIE 7.0b; Windows NT 6.0). יצוין כי ה-User Agent אינו מכיל את התו רווח בין 4.0 לסוגריים מה שמצביע על טעות ביישום או תכנון מכוון לטובת זיהוי ההתקנה של הפוגען בנקודת קצה.
5. שרתי ה-C2 אינם זמינים / מגיבים לשידור הפוגען כעת.
6. השידור מבוצע באמצעות הזרקת קוד ל-iexplore.exe. טכניקה מקובלת לטובת הסוואת ההתקשרות החוצה בפני תוכנות הגנה אשר מותקנות על תחנת הקצה.

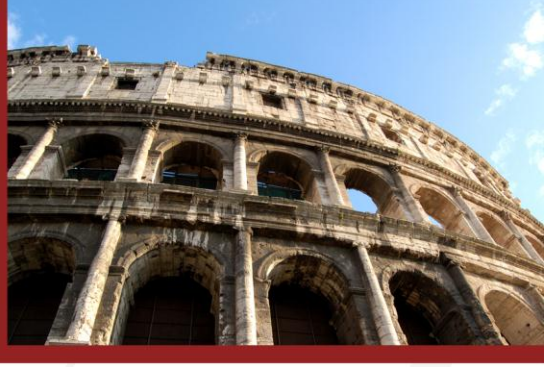
## 3. מקור הקובץ

1. כתובת ה-IP אליו משדר הפוגען נמצא ברוסיה.
2. טווח כתובות ה- IP שימש בעבר שרתי bot בעלי מקורות בשוק הדיגיטלי הפיראטי ברוסיה.
3. הדומיין אליו משדר הפוגען נרשם ע״י Power Holding Corporation במינכן. ככל הנראה מדובר בחברה פיקטיבית שכן נעשה שימוש במייל פיקטיבי לצורך רישום הדומיין.

```
 Power Holding Corporation
Power Holding Corporation        (hgfrfv@yahoo.com)
L L LANE
3
Munich
Bayern,80111
DE
Tel. +49.419199102912

Creation Date: 15-Oct-2012
Expiration Date: 15-Oct-2013

Domain servers in listed order:
    ns1.green-mean.com
   ns2.green-mean.com
```



## 1. המלצות ראשוניות

1. עדכון תכנת האנטי וירוס בתחנות הקצה. הפוגען מזוהה כיום ע"י מרבית חברות האנטי וירוס לרבות Symantec, Kaspersky ו-Mcafee.
2. עדכון רשומת ה-DNS לשרתים המוזכרים מעלה אל הכתובת 127.0.0.1. העדכון יכול להתבצע במס' שיטות, לדוגמה:
   א. הוספת רשומה רלוונטית בשרתי ה-DNS.
   ב. עדכון קובץ ה-Hosts על כלל מחשבי הקצה והשרתים.
3. מניעת חיבורים ל-URI המכיל /portal1/gateway.php
4. מניעת חיבורים עם User Agent המכיל Mozilla/4.0(compatible; MSIE 7.0b; Windows NT 6.0) (ללא רווח בין האפס לפתיחת הסוגריים)
5. ניטור הדבקה קיימת / הדבקת עבר ע"י ניתוח הדפוסים אשר צוינו ונסקרו במסמך זה.
6. שיפור מענה ההגנה הארגוני להגנה על תחנות מסוג זה ע"י הקשחה ממוקדת של התחנה (כולל White Listing מלא) , הקשחת שימוש בהתקנים חיצוניים, צמצום ומיקוד אמצעי התקשורת החוצה של התחנה ובצוע ניטור פרואקטיבי.

## 2. סיכום

1. נראה כי המתקפה אינה מהווה פריצת דרך בהיבטים הטכנולוגיים. לא הושקעו מאמצים ניכרים בבניית הפוגען וטכניקות ההסוואה נחשבות לסטנדרטיות בקרב פוגענים מסוג זה. יתרה מכך, דפוס השידור קל לזיהוי משום שהוא מכיל User Agent שאינו קיים.
2. עם זאת, מדובר במתקפה ממוקדת ואפקטיבית אשר דרשה רמת תפעול (זיהוי המטרות, החדרה, הדבקה, ניהול המבצע) בעלת מורכבות שאינה נמוכה והנחשבת לבינונית.
3. תקן PCI DSS אשר מטרתו הגנה על נתוני כרטיסי אשראי בכלל ועל תחנות תשלום בפרט, לא בהכרח היה מונע את המתקפה היות ומדובר במתקפה ייעודית ללא חתימה ידועה ואשר תוקפת את הפסים המגנטיים בעודם נמצאים באופן גלוי בזיכרון הנדיף של התחנה (לא מכוסה במסגרת תקני PCI DSS ו- PA DSS).
4. ניתן לראות במתקפה מסוג זה משום קפיצת מדרגה נוספת ברמת התחכום והאוטומציה של מתקפות מתחום הפשע הקיברנטי במיקוד על גניבה של פסים מגנטים באופן יחסי למתקפות "המסורתיות" של קוראי שפתיים וכד'.

© **הודעה בדבר זכויות יוצרים:** אין להעתיק, לשכתב, לצלם או לשלוח מסמך זה או חלקים ממנו מבלי לקבל אישור בכתב מחברת קומסק. המידע המופיע במסמך זה הנו רכושה של חברת קומסק ומותר לשימושו הבלעדי של לקוחות קומסק. כל הקורא מסמך זה, כולו או מקצתו, ואינו מורשה למידע המופיע בו, חשוף לתביעה משפטית. המוצא מסמך זה מתבקש להעבירו לידי חברת קומסק.