01 אפריל 2015
י״ב ניסן תשע״ה
סימוכין: ל-ס- 092

<u>הנדון: מידע היערכותי לקראת תקיפה אנטי-ישראלית "OpIsrael#" בסייבר ב- 7 באפריל 2015</u>

<u>רקע</u>

"מבצע OpIsrael"[1] הינה פעילות התקפית אנטי-ישראלית מתואמת במרחב הסייבר, המתבצעת על ידי מספר קבוצות האקרים מרחבי העולם בתאריך ה-7 באפריל (המועד עליו הכריזו בפומבי קבוצות אלו), כל שנה מאז שנת 2013.

קבוצות אלו מזהות עצמן עם קהילת האקטיביסטים Anonymous[2] ועל פי רוב, מעשי הפשיעה בסייבר שהן יוזמות במהלך פעילותן מיועדים ליצירת הד תקשורתי, הפחדת הציבור והעברת מסרים פוליטיים.

לאור ניסיון העבר מהשנתיים האחרונות, פעילות זו התרחשה בימים שלפני ואחרי מועדה הפומבי של התקיפה ב- 7 באפריל, לפיכך, עולה הסבירות כי גם השנה מתקפה זו תתפרס על פני מספר ימים.

<u>סוגי תקיפות</u>

במסגרת פעילות זו ישנן מספר סוגי תקיפות נפוצות (כאשר לכל אחת מהתקיפות מגוון רחב של דרכים וכלים לביצוע), להלן:

- התקפות מניעת שירות (DoS)[3] ובפרט התקפות מניעת שירות מבוזרות (DDoS)
- חדירה למאגרי נתונים והדלפת מידע
- תוכנות כופר (Ransomware)[4]
- השחתת אתרים (Defacement)[5]

<u>יעדים לתקיפה</u>

יעדי התקיפה הטיפוסיים על בסיס מתקפות קודמות הם אתרי ממשל, בנקים, אוניברסיטאות, עמותות, עסקים קטנים, עיתונים בישראל ואף משתמשים פרטיים. בשנים עברו היקף הפגיעה היה שולי יחסית,

[1] Wikipedia - opIsrael
[2] אנונימוס- ויקיפדיה
[3] התקפת מניעת שרות (DoS) - ויקיפדיה
[4] תוכנות כופר (Ransomware) – www.israeldefense.co.il
[5] השחתת אתר אינטרנט (Defacement) - ויקיפדיה

והתקיפות שנצפו לא היו ממוקדות. אולם, אין לכך כל ערובה ויתכן כי בחסותה של פעילות זו יבצעו התוקפים תקיפות ממוקדות נגד ארגונים או יעדים ספציפיים.

סימנים מקדימים לתקיפה

בשבועות האחרונים, מזוהה התארגנות לקראת מתקפה בהיקף נרחב ואנו עדים למספר סימנים מקדימים במרחב הסייבר הישראלי:

1. **פרסום הודעה פומבית ברשת**

כדוגמאות לפרסום הפומבי ניתן להתייחס להודעות להלן. בחודש דצמבר 2014, פורסם בשמם של קבוצת התוקפים AnonGhost סרטון בשם "Cyber Saudi #OpIsrael 7/4/2015"[6], הקורא לפתיחת סבב תקיפות ב-7 באפריל 2015. כמו כן, הודעה ברוח דומה פורסמה בדף הטוויטר "OpIsrael"[7].

2. **הדלפת מידע שנגנב בפריצה למאגרי נתונים**

בשמה של קבוצת התוקפים "AnonGhost" פורסמו הודעות באתרי שיתוף שונים, בהן צוינו כי חבריה פרצו למאגרי נתונים ישראליים וכי בכוונתם להדליף ב- 7 באפריל את המידע שנגנב במסגרת פעילות "OpIsrael#". כמו כן, בתקופה האחרונה מפורסמות רשימות הכוללות שמות משתמש, סיסמאות ופרטי כרטיס אשראי כביכול של ישראלים. בעוד שמרבית הפרסומים מכילים פרטים שגויים או לא עדכניים המיועדים לצבירת הצלחה תודעתית בלבד, מיעוטן של הרשימות מכילות מידע אותנטי.

3. **פריצה מקדימה לאתרים ישראלים והשחתתם**

בזמן האחרון מורגשת עלייה בניסיונות של קבוצות האקרים עצמאיות להשחית עשרות אתרי אינטרנט ישראלים שונים, עד כה בהצלחה מוגבלת מול אתרים קטנים בלבד. אפשר, כי מדובר בפעילות מקדימה לקראת "OpIsrael#".

כלי תקיפה אשר שימשו בהתקפות קודמות

כלי מניעת שירות (DoS)

- **LOIC**[8] – משמש לביצוע מתקפת מניעת שירות מבוזרת (DDoS) על ידי צירוף מספר רב של תוקפים במקביל להצפת TCP או UDP המיועדות ליצור עומס על חומרת השרת הנתקף.
- **HOIC** – כלי מקביל ל-LOIC. מאפשר לתקוף באמצעות הצפת HTTP ומכיל אמצעים להגברת אפקטיביות התקיפה כמו רשימה מתחלפת של עד 256 יעדים מותקפים.

[6] https://vid.me/Ucbf
[7] https://twitter.com/op_israel
[8] Wikipedia - LOIC

- **Anonymous External Attack** – כלי שורת פקודה הבנוי בשפת C#, המשמש להצפת הקורבן ב-4096 חבילות מידע (packets) בשנייה.
- **ByteDos** –משמש לתקיפות הצפת SYN ו-ICMP, המיועדות ליצור עומס על חומרת השרת הנתקף.
- **Snake Bite** – משמש לתקיפות הצפת SYN, המיועדות ליצור עומס על חומרת השרת הנתקף.
- **PyLoris** – משמש לניצול חולשת SlowLoris: פתיחת מספר רב של התקשרויות TCP מלאות במקביל על מנת לחרוג ממגבלת התוכנה של השירות הנתקף.
- **Anonymous Doser**, **BerBoToss Moroccan Attacker**, **DoSHTTP** – כלים שונים לתקיפת יעד בודד באמצעות הצפת HTTP.

<u>כלי הזרקת SQL</u>

- **Havij** - מאפשר סריקה אוטומטית של אתרים לאיתור וניצול חולשות SQL.

<u>הנחיות אבטחת מידע מומלצות:</u>

א. ישנם מספר דרכים להתמודד עם מתקפת DDoS/DoS, כדי להתמודד עם מתקפות מניעת שירות DoS, מומלץ לארגונים לקדם מענה מול מתקפות מניעת שירות באמצעות שירותים הניתנים על ידי גופים שונים בישראל, הכולל פתרונות לזיהוי והפחתת מתקפות נפח ו\או שימוש במוצרים בתחום זה. להרחבה בנושא ניתן לקרוא בקישור הבא:

A Cisco Guide to Defending Against Distributed Denial of Service Attacks

ב. **התמודדות עם תקיפות אתרים:**

1) יש לבצע באופן שוטף עדכוני אבטחה לשרתי ה- WEB ולמערכות ההפעלה.

2) במקרה של שימוש במערכות CMS (Content Management Systems) נפוצות, כגון Wordpress, Joomla, Drupal וכו'. מומלץ לבדוק את הגרסה המותקנת ובפרט את גרסותיהם של התוספים (Plugins) (בהם מצויות רוב החולשות). לבדוק האם קיימת חולשה ידועה להם ולהתקין את עדכון האבטחה שהופץ עבורה. ככלל, מומלץ מאוד לעדכן לגרסה האחרונה שהופצה. כמו כן חשוב לבצע עדכון גרסאות לתוכנות אפליקטיביות מסוג Flash, Adobe Reader, Office, Java וכדומה.

3) יש לבדוק את תקינותם של שדות הקלט באתר ולוודא כי אינם מאפשרים הכנסת תווים שאינם נדרשים או תואמים את הערכים הצפויים.

4) להפעיל ניטור לוגים (Logs) על שרת ה-WEB לאיתור פניות חריגות ובכדי לאפשר יכולת זיהוי תקיפות בדיעבד.

5) לוודא כי ה-Firewall החיצוני מגן על השרתים ומאפשר גישה רק בפרוטוקולים המתאימים.

ג. התמודדות עם פוגענים למחיקת/הצפנת נתונים (Ransomware/Wipers):

1) לוודא קיומו של AV מעודכן.

2) מומלץ שמערכות סינון הדואר יחסמו כניסת קבצי הרצה כגון סיומות EXE, MSI, CAB, BAT וכדומה.

3) להדריך ולחנך את העובדים לאבטחת מידע. להגביר את המודעות באופן כללי ובפרט בזמן זה. לא להתפתות לפתוח הודעות מגורמים לא מוכרים או קבצים חשודים.

4) לחדד את נהלי אבטחת המידע ואכיפתם.

5) לבדוק כי מערך הגיבוי פועל ועובד בצורה תקינה. במידה ולא קיים גיבוי, לבצע גיבוי ולאחסנו במקום מוגן. לרענן את נהלי השחזור של הגיבויים המקוריים, ואף לערוך ניסוי מצומצם לשחזור מגיבוי לבדיקת תקינות הגיבויים.

ד. הנחיות כלליות נוספות:

1) להקשיח את מערכות הפעלה של תחנות העבודה, שרתים וציוד תקשורת לפי הנחיות יצרן.

2) לבדוק כי כל תחנות העבודה והשרתים עם מערכת הפעלה Windows מעודכנות בעדכוני האבטחה האחרונים ומותקנת מערכת אנטי-וירוס, ותאריך החתימות מעודכן לתאריך האחרון.

3) להסיר הרשאות מיותרות במערכות הפעלה ואפליקציות, במיוחד את הרשאות מנהל המערכת Administrator . להסיר חשבונות ברירת מחדל (Default accounts).

4) לשנות סיסמאות בתחנות, שרתים וציוד רשת לסיסמאות מורכבות בעלות 14 תווים ויותר הכוללות: תווים גדולים וקטנים, ספרות וסימנים מיוחדים, כמו כן מומלץ להחליף סיסמה בטווח של 30-90 ימים.

5) להפעיל לוגים בשרתים ואפליקציות ולנטר אותם בתכיפות גבוהה יותר לממצאים חשודים.

6) להגביר את פעילות הניטור במערכות השונות (FW, IDS, IPS, SIEM, AV וכיו"ב), בדגש על סוגי התקיפה שצוינו.

7) לוודא שאפליקציות WEB תומכות לפחות ב-OWASP Top10 להרחבה בנושא ניתן לקרוא בקישור הבא: https://www.owasp.org/images/c/cd/OWASP_Top_10_Heb.pdf

8) לרענן את התוכנית האירגונית להתאוששות מאירוע סייבר. אם לא קיימת כזו, זהו הזמן ליצור אותה.

9) לחדד את המודעות הארגונית הכללית לאבטחת מידע, כמו גם לסימנים העשויים להעיד על תקיפת סייבר על רשתות הארגון.

10) להרחבה בנושא התגוננות אישית ניתן לקרוא בקישור הבא: 10 הדיברות להתגוננות אישית באתר CERT-IL.

בברכה,

ה-CERT הלאומי
טל: 03-7450801
team@cert.gov.il
www.cert.gov.il