דו"ח מעבדה- תרחיש מס' \_01\_

# פרטים:

מגיש: **ברק שרעבי**

תאריך:01.11.18

שם התרחיש: **Shutdown**

# תהליך הזיהוי:

תהליך הזיהוי הראשוני התבצע באמצעות תוכנת ה- ArcSight שיודעת לנתח לוגים מכמות גדולה של שרתים ובהתאם לחוקים שהוגדרו מתריע על חריגות.

בשעה 7:13 UTC לערך התראה ראשונית התקבלה בתוכנה והתריעה על כתובת IP 199.203.100.231 המנסה לגשת למקום אסור 130.2.1.21 שזוהי כתובת IP של שרת אפצ'י האחראי על אתר FOXNEWS.

זאת התבצע על פי תוכנת ה Nmap למיפוי פורטים פתוחים ולחדירה דרכם.

# תהליך ההתקפה:

לאחר תהליך ההתקפה הארגון חווה קושי בגישתו לאתר Foxnews וזאת לאחר שניסה להרים את התהליך בחזרה הוא הבין שמהות התקיפה הייתה כנראה אחרת.

# תהליך הגנה:

תהליך ההגנה הראשוני באירוע מסוג זה הוא חקיקת חוק חדש למניעת תקשורת בין "האקר" לשרת הארגון. זאת עושים באמצעות תוכנת Smart view Tracker של חברת צ'ק פוינט.

חוק ראשון שנחקק הוא אי מתן גישה לכתובת הIP לעיל לתוך הארגון.

חוק שני שנחקק חסימת כל היציאות של השרת לתקשורת עם התוקף.

# תהליך הגנה מונעת:

לשם הגנה על הארגון לחקור את הקובץ שהושתל לתוכה תוך כדי שינוי סיסמאות הארגון והפקת הלקחים.

# הפרצות באבטחת הארגון

# כלים שפיתחנו

# אופן עבודת הצוות :

הצוות חווה קושי בשיתופי פעולה למיגור התקיפה וזאת בשל חוסר ידע, ניסיון והכרות עם התוכנות השונות.

על הצוות ללמוד לעבוד בשיתוף פעולה יחד עם מתפעל האירוע וכמובן לצבור ניסיון וידע בתוכנות השונות על מנת לעצור את התקיפה הבאה.

הצעות ייעול – על הצוות בזמן תקיפה לשבת ולחלק עבודה כדי לייעל את תהליך ההגנה.

# חוסרים/קשיים

הקשיים הבולטים באירוע מסוג זה הוא חוסר היכרות עם מצבים אלו, סנכרון בין כל עובדי הארגון ובעיקר חוסר ניסיון וידע בתפעול אירועים מסוג זה.