דו"ח מעבדה- תרחיש מס' _02_

פרטים :

מגיש : ברק שרעבי

תאריך : 15/11/18

שם התרחיש: Web Defacement

תהליך ההתקפה :

תהליך ההתקפה התבצע באמצעות Port-Scanning

התוקף ביצע סריקה לכל הפורטים הקיימים ולכל אחד מהם שלח בקשה לבדיקה האם יקבל איזשהו תשובה,

בכך התוקף הצליח למצוא פרצה לאחד מן הפורטים שהוא פורט הSSH (22) ומצא "אוזן קשבת"

לאחר מכן הפורץ עשה Brute Force ל ROOT ובכך הסיסמא נפרצה והצליח לגשת לשרת.

לאחר הפריצה ה"האקר" ביצע שינוי\הוספה בתיקיה הנמצאת בנתיב (var/www/html) נתיב זה מאחסן את התיקייה ובה נמצאים קובצי ה index של אתר האינטרנט שלנו ושם הוסיף תיקיה חדשה בשם (BBC)המאחסנת קבצי Index שהתוקף יצר.

לאחר מכן האקר ניגש לנתיב (etc\apache2\site-available) לתוך קובץ בשם default קובץ זה אחראי על נתיב ה index שיפתח בעת העלאת האתר ושם שינה את הנתיב מהתיקייה של האתר שלנו לתיקיה של הקבצים שהוא השתיל והתוצאה הייתה מתקפת Web Defacement.

תהליך הזיהוי :

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

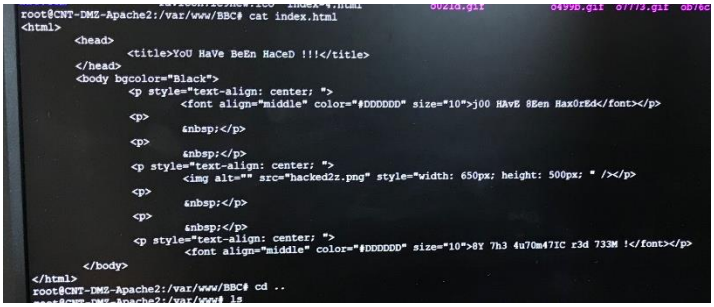
ה- ArcSight התריע על שני מקרים

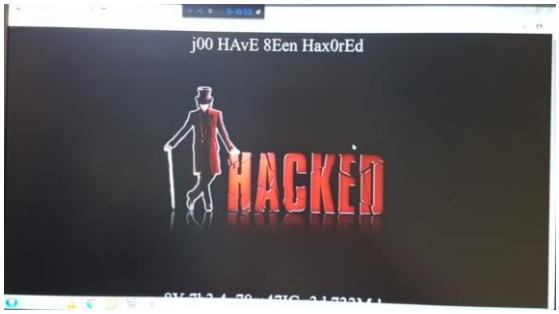
End Time	Name	Attacker Address	Target Address	Priority	Device Vendor	Device Product
UTC 07:03:58 2018 נוב 15	(Elbit) - Password Guessing Detected			7	ArcSight	ArcSight
UTC 07:01:16 2018 נוב 15	(Elbit) - Port Scanning Detected	199.203.100.86	130.2.1.22	7	ArcSight	ArcSight

1. Port-scanning
2. Password guessing detected

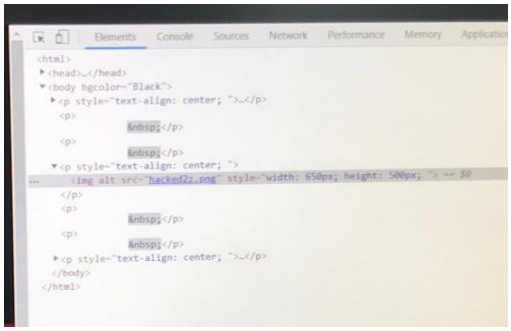
בשעה 7:01 UTC לערך התראה ראשונית התקבלה בתוכנה והתריעה על כתובת IP 199.203.100.86 המנסה לגשת ל - 130.2.1.22 שזוהי כתובת IP של שרת אפצ'י האחראי על אתר BBS.

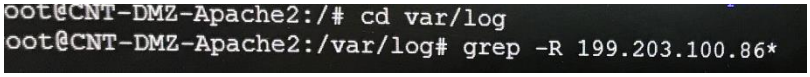
לאחר מכן ניסיון גישה לאתר הראה כי האקר הצליח לגשת לשרת ולהשתיל קבצים.





ניגשנו לשרת Apache וביצענו סריקת רקורסיבית אחר IP של התוקף ובנוסף חיפשנו את אחד מן המאפיינים שהושתלו שזהו התמונה שהאתר העלאה והממצאים הראו כי האקר ביצע שינוי בתיקיית ה html שלנו.





לאחר גישה לתיקייה אבחנו בתיקייה חדשה שהושתלה בנוסף לתיקיה המקורית של האתר ששם נמצאים כל הקבצים המקורים של האתר.

ובנוסף ניגשנו לשירות Apache2 שירות האחראי להעלאתו של האתר ובדקנו את קובץ המיפוי default לראות לאיזה נתיב הוא מפנה.

הממצאים הראו כי הנתיב שונה לתיקייה החדשה שהושתלה ושם נגמר התרחיש.

```
root@CNT-DMZ-Apache2: /etc/apache2/sites-available
    </Directory>

</VirtualHost>
root@CNT-DMZ-Apache2:/etc/apache2/sites-available# nano  default
root@CNT-DMZ-Apache2:/etc/apache2/sites-available# service apache2 restart
 * Restarting web server apache2
 ... waiting .
root@CNT-DMZ-Apache2:/etc/apache2/sites-available# cat default
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        ServerName www.bbc.co.uk
        DocumentRoot /var/www/BBC/
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/BBC/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
                AllowOverride None
                Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>

        ErrorLog /var/log/apache2/error.log

        # Possible values include: debug, info, notice, warn, error, crit,
        # alert, emerg.
        LogLevel warn

        CustomLog /var/log/apache2/access.log combined

    Alias /doc/ "/usr/share/doc/"
    <Directory "/usr/share/doc/">
        Options Indexes MultiViews FollowSymLinks
        AllowOverride None
        Order deny,allow
        Deny from all
        Allow from 127.0.0.0/255.0.0.0 ::1/128
    </Directory>

</VirtualHost>
root@CNT-DMZ-Apache2:/etc/apache2/sites-available#
```

```
root@CNT-DMZ-Apache2:/var# cd www
root@CNT-DMZ-Apache2:/var/www# ls
BBC  BBC_old  hacked!  HACKED!
root@CNT-DMZ-Apache2:/var/www#
```

התיקייה המקורית של האתר

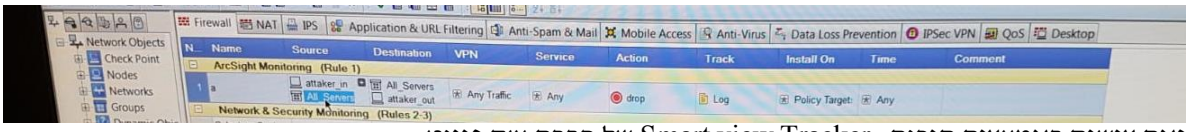
התיקייה שהושתלה

נתיב קובץ ה-default

הגדרת הנתיב אליו יפנה השרת בפתיחת האתר

תהליך הגנה :

תהליך ההגנה התבצע באמצעות חקיקת 2 חוקים חדשים למניעת תקשורת בין "האקר" לשרת הארגון ובין השרת "להאקר"

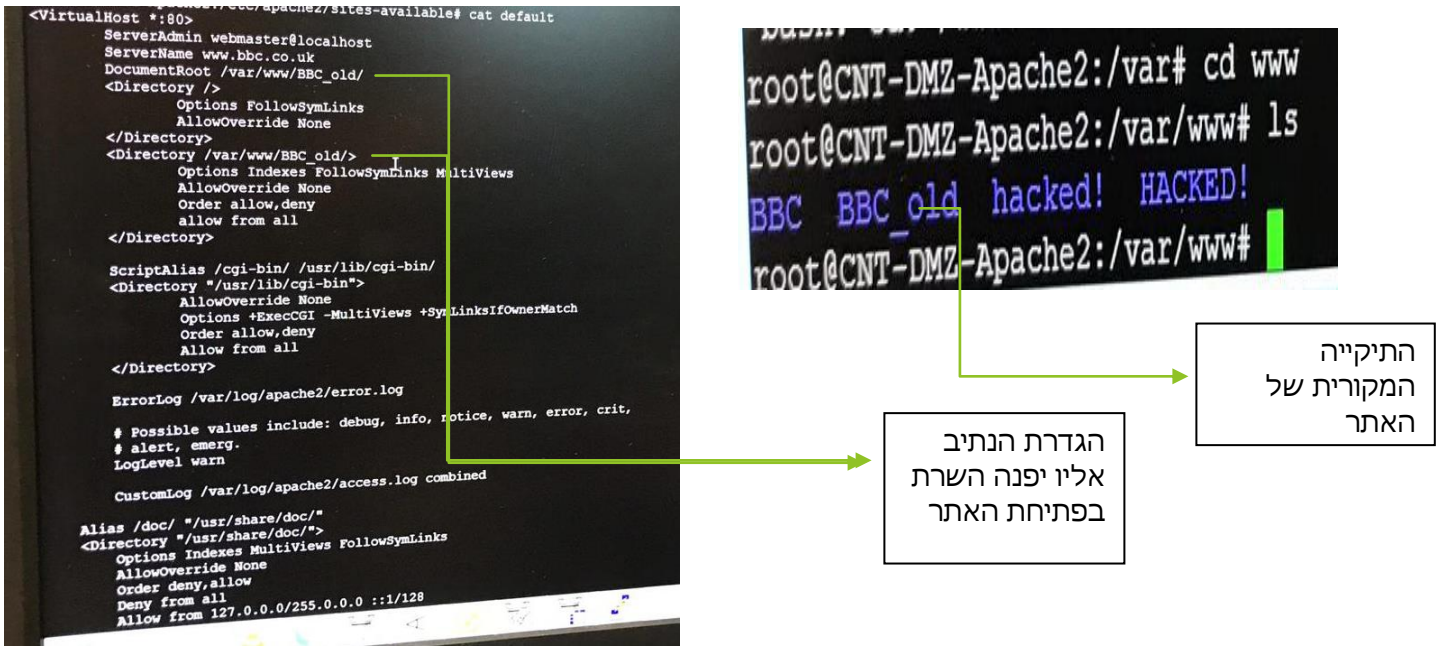


זאת עושים באמצעות תוכנת Smart view Tracker של חברת צ'ק פוינט.

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

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

לאחר מכן ניגשנו לשירות Apache2 לקובץ ה-default וביצענו שינוי מנתיב התיקייה שהאקר שינה לנתיב התיקייה המקורית של הארגון.



את התיקייה של האקר שמרנו במקום אחר לשם חקירה נוספת למניעת "הפתעות"

תהליך הגנה מונעת:

- חסימת גישה ב SSH(22) מחוץ לארגון.
- הרשאות גישה לצוות הארגון בלבד
- חסימת משתמש לאחר מספר ניסיונות
- מתן הרשאות לתיקיות מערכת לעובדי הארגון בלבד
- קביעת מדיניות לחוזק סיסמא

הפרצות באבטחת הארגון

פורט SSH (22) שהייה פתוח ואפשר לתוקף גישה לשרת וביצוע Brute Force ל ROOT

- גישה ב SSH(22) מחוץ לארגון.
- אי חסימת משתמש לאחר מספר ניסיונות
- מדיניות סיסמא חלשה בארגון

אופן עבודת הצוות

לאחר התרחיש הראשון הצוות הצליח לשתף פעולה למיגור התקיפה וזאת בשל אימון, ניסיון והכרות חלקית עם התוכנות השונות.
על הצוות להמשיך וללמוד לעבוד בשיתוף פעולה יחד עם מתפעל האירוע וכמובן לצבור ניסיון וידע בתוכנות השונות על מנת לעצור את התקיפה הבאה.
וזאת באמצעות קריאה ולמידה מורחבת על התקיפות השונות ואופן השימוש בשרת ופקודותיו.
הצעות ייעול – על הצוות לעבוד בשיתוף פעולה וחלוקת תפקידים 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.