יוני 2022

* - מידע לא מאומת

2 ביוני -
חברת **Microsoft** חשפה קמפיין תקיפה המכונה POLONIUM, הפועל מלבנון ותוקף יעדים בישראל (תשתיות קריטיות, תעשיה ביטחונית ו-IT)

2 ביוני -
קבוצה של גולים איראנים ("מוג'אהדין חלק") טוענת לתקיפת מצלמות אבטחה של המשטר באיראן ולהשחתת אתרים משלתיים

4-6 ביוני -
דיווחים תקשורתיים על מותם של שני מדענים איראנים בנסיבות לא ברורות; דיווח תקשורתי על מותו של בכיר ביחידה 840 של כוח קודס

7 ביוני -
קבוצת **JEA** טענה כי בצעה תקיפות על תשתיות אנרגיה וחשמל בישראל*; רומזת לאחריות על גרימה להפסקת חשמל באשקלון*

11 ביוני -
קבוצת **Altharea** טענה כי בצעה תקיפת DDoS נגד אתר הבורסה*

12-14 ביוני -
קבוצת **Sharp Boys** הדליפה מידע אישי רגיש ממספר אתרי תיירות ישראליים אשר נפרצו על ידי הקבוצה

14 ביוני -
חברת **Check Point** חשפה קמפיין פישינג איראני אשר הופנה כנגד בכירים לשעבר בישראל ובארה"ב (חשוד UNC788)

14 ביוני -
קבוצת **Mosses Staff** טענה כי תקפה את חברת החשמל, חברת "דוראד" וחברת מערכות הבקרה Realiteq*

20 ביוני -
שר הביטחון גנץ מצהיר כי ישראל בונה ברית הגנה אווירית אזורית בחסות אמריקאית

20 ביוני -
תקיפות סייבר, החשודות כאיראניות, על מערך האזעקות של מספר רשויות מקומיות (אילת וירושלים)

22 ביוני -
קבוצת **Mosses Staff** טענה לאחריות על התקיפה של מערכות האזעקה של הרשויות המקומיות (20 ביוני)*; טענה לפגיעה פיזית בבלון תצפית של צה"ל בגבול עזה*

23 ביוני -
דיווח על מעצר סוכנים איראנים בתורכיה אשר תכננו לפגוע בדיפלומטים ותיירים ישראלים

25 ביוני -
קבוצת Altharea טענה כי בצעה תקיפת DDoS על אתר משלוחי מזון ישראלי ("משלוחה")*

27 ביוני -
קבוצת **Gonjeshke Darande** טענה כי בצעה תקיפה על שלוש חברות לייצור פלדה באיראן, המזוהות לטענת הקבוצה עם משה"מ והבסיג'

28 ביוני -
קבוצת **GhostSec** הכריזה על השתתפות בקמפיין #OpIsrael, טענה כי בצעה תקיפה על מערכת בקרת קירור בישראל*

28 ביוני -
קבוצת **Sharp Boys** הדליפה מידע אישי רגיש מאתרי התיירות אשר תקפה בתחילת החודש; טענה לתקיפת אתרים נוספים*

קבוצות **1887 Team** ו-**Altharea** טענו לתקיפת DDoS על אתר חברת Cellebrite

29 ביוני -
ארגון **"חיזבאללה"** ניסה לשגר כלי טיס בלתי מאויש לעבר המים הכלכליים של ישראל

שר הביטחון גנץ האשים את איראן וארגון "חיזבאללה" בביצוע תקיפת סייבר כנגד יוניפי"ל; כמו כן, הצהיר כי יחידת סייבר של משה"מ בשם Shaid Kaveh פועלת על מנת להשיג מידע שמטרתו פגיעה בספינות, תחנות גז ומפעלים תעשייתיים

30 ביוני -
קבוצת **GhostSec** טענה כי בצעה תקיפות נוספות על מערכות בקרה (מים וחשמל) בישראל*

* - מידע לא מאומת

יולי 2022 (1)

2 ביולי -

ארגון "חיזבאללה" שיגר שלושה כלי טיס בלתי מאוישים לעבר אסדת הגז "כריש" (בפעם השנייה החודש)

4 ביולי -

קבוצת **Altharea** טענה כי בצעה מתקפת DDoS על אתר חברת נת"ע (האחראית על פרויקט הרכבת הקלה והמטרו בגוש דן)

6 ביולי -

קבוצת **Sharp Boys** טענה כי תקפה 48 אתרים ישראלים, מרביתם פלטפורמות מסחר קטנות וחנויות טבע*

7 ביולי -

קבוצת **GhostSec** טענה כי בצעה תקיפות על מכשירי בקרה אלקטרוניים ומערכות בקרה תעשייתיות (ICS) בישראל*, ביניהם מערכת בקרת משאבות הביוב של עיריית אור עקיבא (זוהה בטעות על ידי התוקף כמערכת גז); קראה לפעילות משולבת כנגד אתרים של גופים ממשלתיים, חברות ממשלתיות ויעדים נוספים

9-10 ביולי -

בכירים איראניים ואתר Nour News, המזוהה עם המועצה העליונה לביטחון לאומי של איראן, הצהירו כי יצירת ברית ההגנה האזורית היא אקט "מאיים";

איראן הצהירה על התחלת העשרת האורניום ל-20% זאת באמצעות צנטריפוגות חדשות הנמצאת במתקן הגרעיני בפורדו

12 ביולי -

קבוצת **GhostSec** דחתה פרסומים תקשורתיים אודות הטענות למעורבות הקבוצה ב"מלחמת הסייבר בין איראן לישראל"; טענה כי המוטיבציה מאחורי התקיפות היא סולידריות עם המאבק הפלסטיני

13 ביולי -

נסראללה נשא נאום במהלכו איים על ישראל, והצהיר כי כלי הטיס הבלתי מאוישים אשר נשלחו לעבר שדה הגז "כריש" היו "רק ההתחלה" וכי "יש הרבה יותר כבוד במלחמה מאשר המקום אליו הולכת לבנון כעת"

2 ביולי -

קבוצת **GhostSec** טענה כי השיגה גישה למצלמת אינטרנט הצופה על כביש בישראל*

4 ביולי -

דיווחים תקשורתיים על מתקפת סייבר כנגד בנקים באיראן*

7 ביולי -

קבוצת **Gonjeshke Darande** הדליפה 20GB של מידע והתכתבויות דוא"ל שהושגו מתקיפת מפעלי הפלדה באיראן ב-27 ביוני (הדלפה ראשונה)

9 ביולי -

קבוצת **GhostSec** טענה כי בצעה תקיפות נוספות על מערכות בקרה תעשייתיות בישראל*

11 ביולי -

קבוצת**Altharea** טענה כי בצעה תקיפת DDoS על אתר עיריית תל אביב

13 ביולי -

ביקור הנשיא ביידן בישראל

* - מידע לא מאומת

יולי 2022 (2)

14 ביולי -

הנשיא ביידן ורה"מ לפיד חתמו על "הצהרת ירושלים", המחייבת את שתי המדינות לעצירת איראן מהשגת נשק גרעיני, ומחייבת את ארה"ב לשמירה על העליונות הצבאית של ישראל;
טקס פתיחת משחקי המכביה

קבוצת **Gonjeshke Darande** הדליפה 10GB נוספים של מידע מתקיפת מפעלי הפלדה באיראן ב-27 ביוני (הדלפה שניה)

Cyberint מפרסמת דו"ח על קבוצת **GhostSec**

15 ביולי -

ביקור הנשיא ביידן בסעודיה;

איחוד האמירויות מציינת כי לא תצטרף לברית האזורית נגד איראן

17 ביולי -

קבוצת **Altharea** טענה כי בצעה מתקפת DDoS על אתר משרד הבריאות, דבר שגרם למניעת הגישה לאתר מחו"ל (כצעד הגנתי)

קבוצת **GhostSec** רמזה כי פרצה לשרת אחסון אתרים ישראלי*

19 ביולי -

הנשיא פוטין צפוי לבקר באיראן, ולהיפגש עם מקבילו הנשיא ארדואן ונשיא איראן ראיסי; ישנם דיווחים גם על פגישתו המתוכננת עם המנהיג העליון ח'אמנהאי

14 ביולי -

קבוצת **Altharea** טענה כי בצעה תקיפת DDoS על אתר עיריית ירושלים; תקיפת DDoS על אתר חברת 'רפאל'*;
כמו כן, טענה כי תקפה מערכת בקרה בתחנת הכוח "אורות יוסף" בנאות חובב, ורמזה לאחריות לשריפה אשר פרצה במקום;
הקבוצה טענה בהמשך כי תקפה מערכות בקרה נוספות בישראל

16 ביולי -

קבוצת האקרים אינדונזית טענה כי פרצה למספר אתרים ישראלים; חלק מהתארים הופיעו ברשימות אתרים שנפרצו בעבר*

קבוצת **Lab Doukhtegan** מדליפה את זהויותיהם של מספר האקרים איראנים המזוהים עם משה"מ

*מידע לא מאומת

תובנות והערכות

- **במהלך החודשים האחרונים, אנו מזהים עליה בכמות האירועים למול תשתיות קריטיות, ארגונים תעשייתיים ומערכות OT/ICS מצד שחקנים מדינתיים. יחד עם זאת, בחודשים האחרונים, התעניינות דומה מזוהה גם בקרב קבוצות אחרות, אשר אינן פועלות בהכרח בחסות מדינתית (למשל, קבוצות האקטיביסטיות).**
  - **מוטיבציה** - בתור הסברים אפשריים למגמה, ניתן לציין את המלחמה באוקראינה ופעילות הסייבר ההתקפית של רוסיה בגזרה; ואת העלייה הגלובלית במחירי האנרגיה, המייצרת תחרות גדולה בשוק האנרגיה ואספקתה. דוגמא נוספת היא תקיפת הכופרה ב-Colonial Pipeline הממחישה גם את הפוטנציאל הכספי הרב שיש לאירוע סייבר המתרחש בסביבה תפעולית, או בסביבת IT הסמוכה לסביבת ה-OT.
  - **שינוי ב-TTPs** - במסגרת האירועים האחרונים, אנו מזהים שימוש בכלים פומביים, למשל במודולים ייעודיים של Metasploit למערכות OT/ICS, וזאת על ידי שחקנים ברמת תחכום נמוכה. מדובר בעדות לכניסתם של שחקנים חדשים לזירה אשר הייתה נשלטת עד כה על ידי שחקנים מדינתיים ברמה מקצועית גבוהה ביותר.

- **<u>ההקשר האזורי:</u>**
  - חקיינות והגברת החומות - תקיפת מפעלי הפלדה באיראן על ידי קבוצת Gonjeshke Darande יתכן ותשמש כטריגר לתגובת-נגד איראנית כנגד ישראל או בעלות בריתה (אשר חשודות במעורבות), יתכן במתווה דומה למול תשתית קריטית או תעשייתית.
  - קבוצות תקיפה שונות, אשר מרביתן מזוהות עם איראן, ממשיכות לטעון לאחריות על תקיפות DDoS ומבצעי Hack & Leak כנגד ישראל (מרבית הטענות אינן אומתו במלואן). אנו מעריכים כי פעילות זאת צפויה להימשך, וכמו כן גם הפעילות למול רכיבי ה-ICS, המתבצעת כעת בעיקר על ידי קבוצת GhostSec.
  - המתיחות סביב אסדות הגז והתגברות האיום הקינטי מצד חיזבאללה, יתכן ויובילו לפעילות נוספת כנגד ישראל במרחב הסייבר, זאת מצד חיזבאללה או מצד קבוצות אחרות הפועלות מלבנון תחת חסות איראנית.
  - צעדים נוספים בקידום הנורמליזציה בין ישראל למדינות האזור וההתפתחויות בשיחות הגרעין עם איראן, יתכן וישמשו כטריגר לפעילות סייבר כנגד ישראל.