**דו"ח יומי** | **מרכז נאס"א**
21.06.2018

|  |
| --- |
| **תקציר מנהלים**• התקבלו **8** פניות חדשות ביממה החולפת, מתוכן **6** פניות מעמיתים בינלאומיים.• הופצו התרעות ב-TLP לבן.• נרשמו **1** אירועים חדשים בגוף ממשלתי.• נרשמו **0** אירועים חדשים בגופי תמ"ק.• נרשמו **8** אירועי השחתה. |

אירועים פתוחים

Sddds

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| נמוך |  | קריטי | **תאריך קבלה:**20.06.18  | חשד לאירוע בכנסת | **חדש** | **1** |
|  התקבל דיווח טלפוני מאיש אבט"מ בכנסת, אודות חשד לבוטנט במס' עמדות בכנסת. לדבריו, ה-IPS שלהם (של צ'קפוינט) התריע על כך שיש להם מס' תחנות המשמשות כ-BOT, ה-IPS מציין זאת כ-bot incident.העמדות הנ"ל ניסו לבצע שאילתות DNS לשרתי C&C בין ה-31.5-7.6, אך מאחר והתקשורת של הכנסת עוברת דרך תהילה הבקשה נחסמה שם. תהילה טענו כי נצפו פניות זהות בעוד מס' משרדים (לא פורט מעבר לכך). תהילה מסרו להם כי הם ראו את ייתכן ומדובר בתוסף של כרום, המזריק נתונים לשם התקשרות לדומיין החשוד. מתחקור נוסף של איש הקשר התברר כי מתוך 15 העמדות הנגועות, שלוש הינן עמדות 'מוקדן' בעלות הרשאות גבוהות משאר העמדות. באחת מעמדות המוקדן הנגועות התגלה שירות המאפשר שיתוף חיבור אינטרנט בין מחשבים המחוברים לאותו מתג, ובמידה וקיים במחשב הנ"ל אמצעי גלישה כלשהו אז יש אפיק גישה ממחשבים אלו למשאבים חיצונים ללא בקרה. עמדה זו פורמטה. |
| **פעולות להמשך:** נשלח דו"ח סיכום ביניים והמשך החקירה. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| נמוך |  | קריטי | **תאריך קבלה:**18.06.18  | נסיונות תקיפה על נתבי D-link | **עדכון** | **2** |
| התקבל דיווח אודות תקיפות על נתבי D-link ביתיים במהלך הימים האחרונים. התקיפה מתבצעת באמצעות גלישה למספר אתרים אשר כניסה אליהם מורידה payload לנתב ובכך הופכת אותו לחלק מתשתית botnet. המידע הועבר לחדמ"צ במטרה שהנ"ל יוציאו חתימות לצורך הפצה לגורמים הרלוונטיים. |
| **פעולות להמשך:** חקירת ה-payload להוצאת ממצאים נוספים לצורך הפצת דו"ח והתרעה. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| נמוך |  | קריטי | **תאריך קבלה:**14.06.18  | התחזות למנכ"ל | חברת יאסקווה | **עדכון** | **3** |
| התקבל דיווח ממנכ"ל חברת יאסקווה (חברת בת של חברה יפנית גדולה YASKAWA Electric Corporation רובוטיקה ואוטומציה תעשייתית) אודות התחזות. דווח כי מנהלת הכספים שלו קיבלה מייל כביכול ממנו. בתוכן המייל, התבקשה להעביר 95,400$ להונג קונג למטרת מימון של מחקר ופיתוח מוצרים לחברה. כמו כן, התגלה שינוי חוק למיילים ממנהלת הכספים, אשר גורם לכך שכל המיילים שמתקבלים ממנה ישמרו בתיקייה מסוימת. מהמיילים המקוריים שהתקבלו לחקירה עלה כי ייתכן ומדובר בפריצה לתיבת המייל של המנכ"ל. נשלחו טפסים משפטיים לחתימה וכן איש הקשר התבקש להעביר את הלוגים של תיבת המייל לחקירה. בנוסף, איש הקשר ציין כי נמצא מייל פישינג בחברה וכי לא ידוע האם נפתח. המייל המקורי הועבר לחקירה, נוסף על מייל ב-forward. |
| **פעולות להמשך:** המשך חקירה. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| נמוך |  | קריטי | **תאריך קבלה:**12.06.18  | חולשות באתר citypay |  | **4** |
| התקבל דיווח אודות חולשה אפשרית באתר Citypay.co.il – פורטל תשלומים לעיריות. מדובר בחולשת SQL Injection. בוצע דיווח לחברת one1 שאחראית על האתר והנ"ל חסמה את האפשרות לבצע תקיפה מסוג זה. במקביל, החברה עובדת על הסרת הפגיעות באופן יסודי יותר. |
| **פעולות להמשך:** קבלת דו"ח חקירה מהחברה לאחר סיום הטיפול באירוע. |

S

 אירועים במעקב

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| נמוך |  | קריטי | **תאריך קבלה:** 28.05.18  | פריצה וניסיון הונאה | חברת NovellusDx |  | **6** |
| התקבל דיווח מחברת NovellusDx אודות פריצה לתיבת דוא"ל של עובד בחברה וניסיון להוציא במרמה 2 מיליון דולרים מאחד מלקוחות החברה, תוך שימוש בפריצה לתיבת הדוא"ל של עובד החברה. בנוסף להתכתבויות מתיבת עובד החברה, נעשה שימוש בדומיין המתחזה לכתובת המנכ"ל. ההעברה הבנקאית לא התבצעה. בוצעה פנייה למשטרה לבדיקת סטאטוס הטיפול בתלונה הקודמת. נמסרו לחברה שתי כתובות IP בבקשה לניטורן בלוגים אך לא עלו ממצאים חשודים. |
| **פעולות להמשך:** בחינת העברת האירוע למשטרת ישראל מאחר ומדובר בהונאה כספית. |

 אירועים סגורים

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| נמוך |  | קריטי | **תאריך קבלה:**19.06.18  | פגיעויות אפשריות בבנק המזרחי ובפניקס | **עדכון** | **7** |
| התקבל דיווח מאזרח אודות פגיעות להתקפת ROBOT אשר מתגלית ע"י סריקה בכלי sslabs וכן אתר של הפניקס אשר מפנה לאתר אחר של החברה אך ללא תעודת אבטחה. הדיווח הועבר ל-SOC הפיננסי. |
| **סיבת הסגירה:**  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| נמוך |  | קריטי | **תאריך קבלה:**18.06.18  | כתובות IP חשודות מקניה | **עדכון** | **8** |
| ה-CERT הקנייתי דיווח אודות שתי כתובות IP חשודות כחלק מתשתית תקיפה על אתרים בארצם. מבדיקה, עולה כי הלוגים מציינים את כתובת ה-IP מקושרת לדומיין מאירוע "נסיונות תקיפה על שרתי D-Link" המשמש להפצת הפוגען.  |
| **סיבת הסגירה:**  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| נמוך |  | קריטי | **תאריך קבלה:**20.06.18  | השתלטות על דומיין של חברת ביטוח- תלפיות | **חדש** | **9** |
|  נתקבלה פנייה מעובדת בחברת הביטוח תלפיות. היא עדכנה כי גורם כלשהו השתלט על דף הנחיתה של החברה, אשר מפנה כעת לדף המכיל חומר פורנוגרפי. אין לחברה עוובדים המתפעלים את האתר באופן סדיר. הומלץ לה לפנות לחברת האחסון על מנת להסיר את הדף, שכן החברה אינה מעוניינת להמשיך לתפעל את האתר. |
| **סיבת הסגירה:** נשלחו המלצות, הדף שוחזר. |

 בברכה,