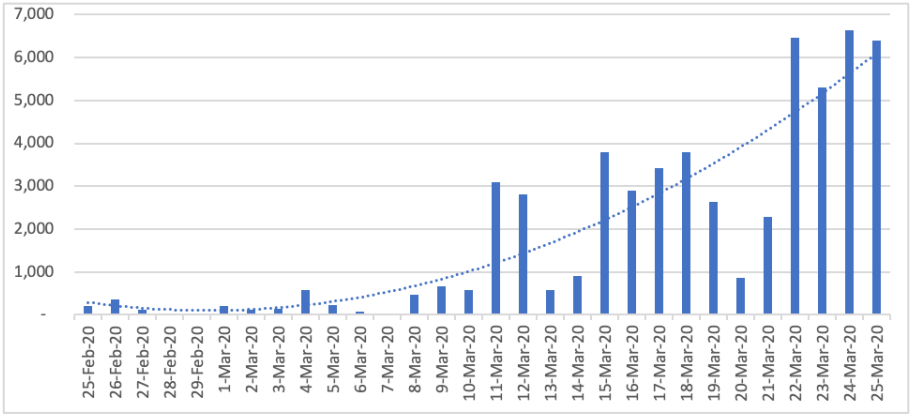
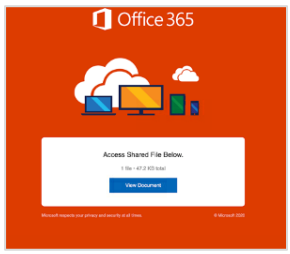
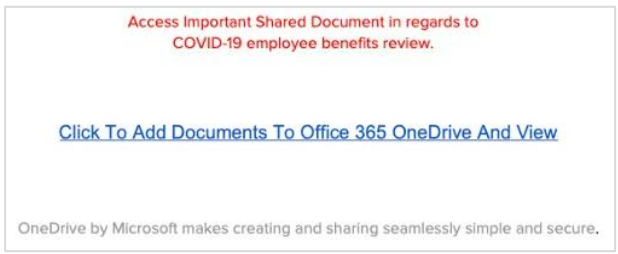
07 אפריל 2020
י"ג ניסן תש"פ

תקיפות דיוג מתוחכמות בנושא נגיף הקורונה, עושות שימוש בצרופות מסוג PDF וטפסים המתארחים בשירותים מוכרים ולגיטימיים (SaaS) על מנת לעקוף הגנות. בחברת Menlo Security גילו כי התקיפה הינה רב שכבתית. הנתונים מראים כי תקיפות המנצלות את נגיף הקורונה וקמפיין דיוג בנושא זה הופכים למוצלחים יותר, לכך נושא משבר הקורונה מהווה פלטפורמה מוצלחת לניצול. החברה מציגה עלייה של פי 32 בתקיפות דיוג מוצלחות בכל יום בחודש שבין 25 לפברואר ועד ל- 25 למרץ השנה.



בנוסף לכך, הדיווח מביא דוגמאות של תקיפות דיוג שונות כמו מסמכי PDF (כאמור), דוא"לים אישיים מטעם דרג ניהולי בכיר ועוד.





קבוצת התקיפה DarkHotel ניצלה שימוש בחולשות מוצרי - VPN. ממשלת סין החלה להשתמש רבות ב-VPN על מנת להעניק גישה למקורות רשמיים במדינה, עבור האנשים שעובדים מרחוק. קבוצת התקיפה ניצלה את ההזדמנות לתקוף את אותם שרתים בתקיפות יום אפס (Zero Day). על פי הדיווח התקיפה השפיעה גם על סוכניות סיניות במדינות רבות בעולם כמו אפגניסטן, אתיופיה, הודו, אנגליה ועוד. הרחבה בקישור.

תוקפים מנצלים את הפופולריות של אפליקציית ZOOM על מנת להפיץ קבצי התקנה לתוכנות המתחזות לאפליקציה המקורית וזאת כדי להפיץ נוזקות. סוגי הנוזקות מגוונים, כדוגמת כורה מטבעות וירטואליים, טרויאני גישה מרחוק ועוד. פרטים נוספים בקישור.

אפליקציית ZOOM הינה אחת מיני אפליקציות שיתוף רבות הקיימות היום. בשל הפרסום הרב בנושא הפגיעויות ובעיות האבטחה הקשות של אפליקציית ZOOM חשוב שלא לשכוח את אפליקציות השיתוף האחרות הקיימות והסיכון הקיים בשימוש גם בהן.
ככל שנמשך משבר הקורונה העולמי והעבודה מהבית נשארת צורת הגישה המרכזית לארגון, כך הולך וגובר הצורך בשימוש באפליקציות שיתוף נוספות כמו Webex, Microsoft Teams ועוד. עם זאת, חשוב לזכור כי בכל אחת מאותן אפליקציות קיימת סכנה, בין אם מדובר בחדירה לפרטיות או לחילופין ניצול חולשה או שימוש בהנדסה חברתית על מנת לבצע מתקפת דיוג ועוד.
הרחבה בקישור.

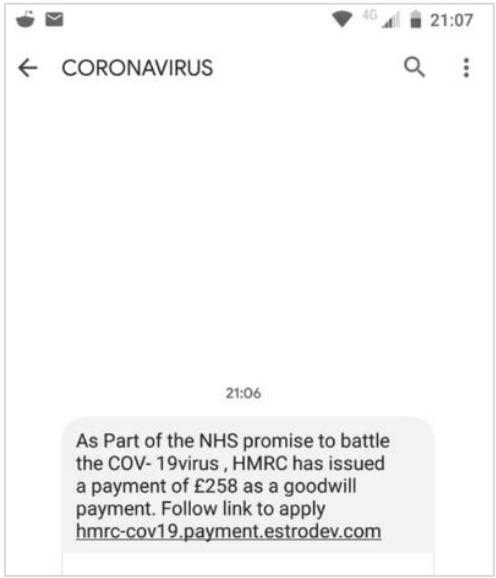
קבוצת התקיפה SideWinder מוציאה לפועל קמפיין תקיפה כנגד פקיסטן, בנושא נגיף הקורונה.

בסוכנות החלל האמריקאית (NASA) מזהים קפיצה משמעותית בכמות התקיפות כנגד כוח האדם שעובד מהבית. הסוכנות מדווחת כי כמות קבלת דוא"לים דיוג הוכפלה, עלייה גדולה מאוד של מתקפות כופרה על מערכות הסוכנות, חסימת פניות לאתרים זדוניים מתוך המערכת. הרחבה בקישור.

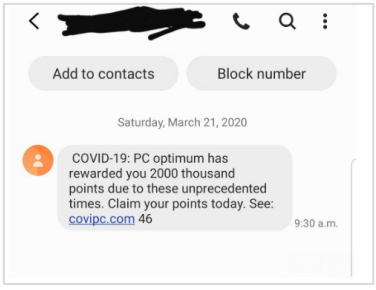
קמפיינים רבים של מתקפות דיוג ממשיכים ומתבצעים ברחבי העולם. להלן מספר דוגמאות מהזמן האחרון:

- דוא"ל דיוג מטעם ארגון הבריאות העולמי

- SMS דיוג עם עדכון לגבי קבלת הטבות כספיות



- SMS דיוג המעדכן לגבי קבלת נקודות לרכישה



- בארצות הברית מתקבלות הודעות מזויפות מ- Amazon כביכול, אשר מבקשות מהמשתמש להתחבר לחשבון על מנת לקבל בקבוק אלכוג'ל מתנה בקנייה הבאה. הרחבה בקישור.

המלצות התגוננות

⇐ לקבלת מידע מהימן ומעודכן אודות התפשטות הנגיף, יש להשתמש אך ורק באתרים רשמיים, כגון אתר משרד הבריאות.

⇐ אין להשיב למסרונים הנשלחים כביכול ממשרד הבריאות אולם מכילים פנייה כללית. מסרונים לגיטימיים הנשלחים מטעם משרד הבריאות, תמיד יכילו את שמו המלא של הנמען.

1. הודעה לחולה בקורונה
[שם פרטי] שלום,
בהתאם לתוצאות הבדיקה, לפיה חלית בקורונה, מבוצעת חקירה אפידמיולוגית כדי לאתר אנשים שנחשפו אליך.
לצורך השלמת החקירה משתמשים באמצעים טכנולוגיים, לפי תקנות שעת חירום.
המידע ישמש את משרד הבריאות רק למטרה זו וימחק בתום הצורך.
מידע בקישור:go.gov.il/corona
לאימות ניתן לחייג 5400*
בברכה
שירותי בריאות הציבור

2. הודעה למי שאותר כמגע של חולה:
[שם פרטי] שלום
לפי חקירה אפידמיולוגית היית בתאריך [==/==/==] ליד חולה קורונה.
עליך להיכנס מייד לבידוד עד [==/==/==] להגנה על קרוביך והציבור.
אם יש לך חום, שיעול וכו' נא להתקשר למד"א - 101.
מידע נוסף בקישור go.gov.il/corona
לאימות ניתן לחייג 5400*
המידע ישמש רק למטרה זו וימחק בתום הצורך.
בברכה
שירותי בריאות הציבור

⇐ במקרה של עבודה מרחוק מומלץ לקרוא את מסמך המלצות הגנה לארגונים ועסקים לעבודה מהבית שהפיץ מערך הסייבר הלאומי.

⇐ אין לפתוח קישורים או להוריד קבצים אשר התקבלו מגורם שאינו מוכר או שאמינותו מוטלת בספק.

⇐ אין למסור מידע אישי כגון סיסמאות או פרטי חשבון ואין להשיב להודעות המבקשות פרטים מסוג זה.

⇐ הורדת יישומונים יש לעשות אך ורק מהחנויות המקוונות הרשמיות.

⇐ בעת ביצוע רכישה מקוונת, יש לגשת ישירות לאתר ולא ללחוץ על מודעות וקישורים לקידום מכירות.

⇐ יש להשתמש במוצרי הגנה כגון אנטי-וירוס וסינון דוא"ל.

⇐ מתקפות על ה- DNS:

- בדיקת הגדרות הקונפיגורציה של הנתב, כך שיקבל את שירותי ה-DNS שלו ישירות מספק האינטרנט.
- ביטול אפשרות לשליטה מרחוק על הנתב.
- שינוי סיסמא לנתב ובחירת סיסמא חזקה וייחודית, בהתאם להמלצות מערך הסייבר הלאומי.
- שינוי סיסמאות לכלל האתרים והחשבונות בהם נעשה שימוש.

⇐ מתקפות על מכשירי iOS:

- עדכון גרסאות של מערכת ההפעלה וה- Antivirus.
- התקנת פתרונות הגנה החוסמים אפליקציות זדוניות ומגנים על המכשיר מפני גניבת פרטים אישיים, אתרי הונאה ועוד.
- צמצום ההרשאות הניתנות לאפליקציות המותקנות במכשיר, למינימום הנדרש.

⇐ מתקפות VISHING:

- שימוש בהזדהות חזקה (MFA / 2FA) לקבלת גישה לחשבונות דוא"ל
- ייצור מנגנון רב ערוצי לשם השגת גישה מרחוק, לדוגמה, שליחת סיסמה ב SMS ושם משתמש בדוא"ל.
- הרחבה בנושא VISHING בהתרעה של מערך הסייבר הלאומי בנושא.

⇐ מתקפות מפני התחזות:

- הטמעת מנגנון אבטחה DMARC (Domain-based Message Authentication, Reporting and Conformance), המנגנון מקטין משמעותית את הסיכון. המלצות נוספות ומדריך בנושא ניתן למצוא בפרסום של מערך הסייבר הלאומי בקישור.

⇐ מתקפות המנצלות את הפגיעות בשרתי Citrix ADC:

- מומלץ לכל ארגון העושה שימוש בציוד זה, לבחון בסביבת ניסוי ולהטמיע מיידית את עדכוני האבטחה שפרסמה חברת סיטריקס ,בהתאם לסוג הציוד הקיים בארגון.
- במקרה של חשד כי הציוד נוצל לתקיפה טרם התקנת העדכון או הגדרת החוק, ניתן להיעזר בכלי החקירה שפרסמה החברה, אותו יש להריץ מקומית על הציוד או כנגד קובץ מכונה וירטואלית המכיל עותק של התוכנה. ראו בקישור.
- המלצות נוספות בנושא ראו בהתרעה של מערך הסייבר הלאומי.

⇐ מתקפות המנצלות את הפגיעות במערכת ManageEngine Desktop Central:

- מומלץ להתקין את גרסת התוכנה העדכנית, 479.4.10 ,לאחר בדיקות בסביבת ניסוי.

⇐ המלצות נוספות ניתן למצוא בהתרעה שהפיץ מערך הסייבר הלאומי, בנושא מתקפות סייבר המנצלות את בהלת הקורונה.