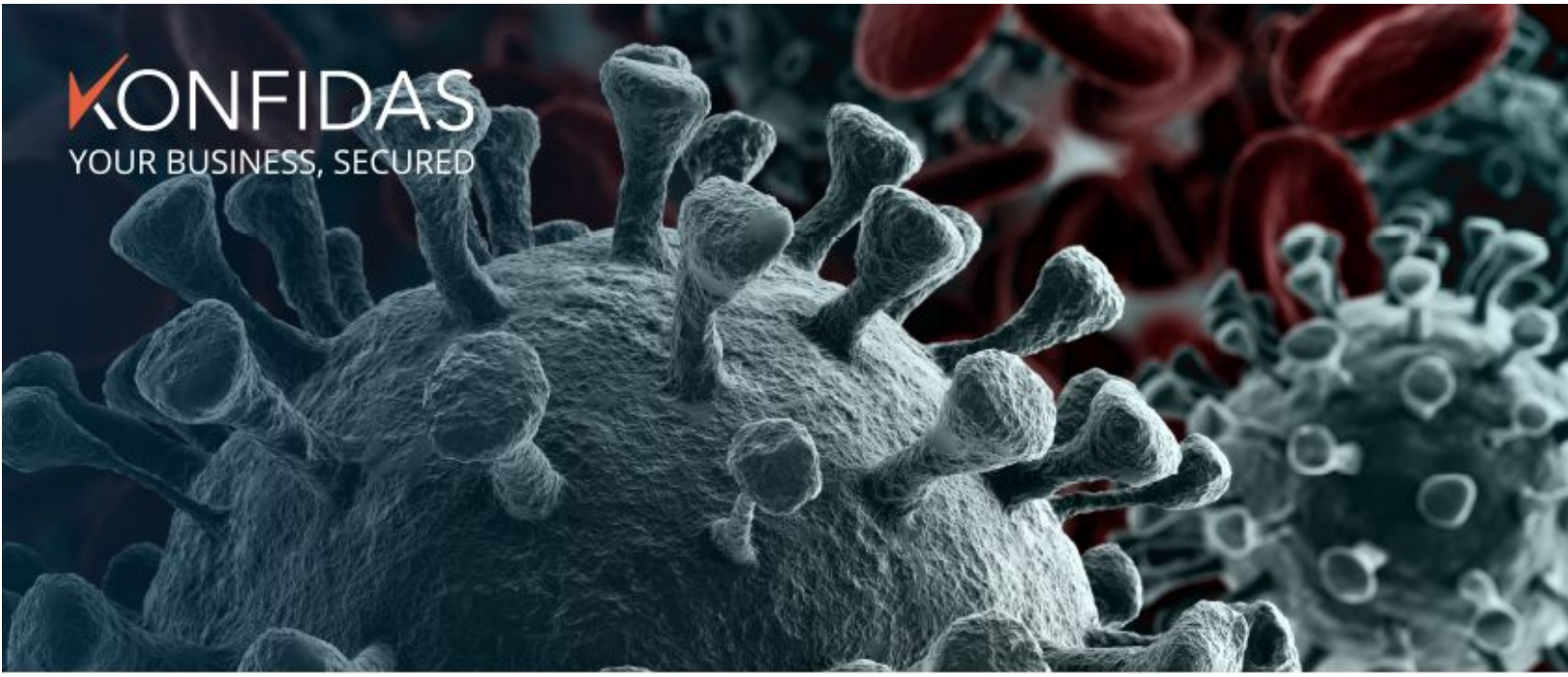


היבטי סייבר ונגיף הקורונה (COVID-19)

עדכון יומי ליום ב׳, 23.03.2020

הדוח היומי מתפרסם גם במדור "קפטן אינטרנט" של עיתון הארץ
https://www.haaretz.co.il/captain

איומים, התקפות והתראות

#1

קמפיין כופרה חדש נעזר בוירוס הקורונה לטרגוט עובדי רפואה למטרות כספיות

קמפיין כופרה מנצל חולשה שנקראת NetWalker (Mailto) במערכת ההפעלה Windows. הקמפיין, אשר מכוון לצוותי הרפואה, התגלה על ידי MalwareHunterTeam ונחקר על ידי Bleeping computer[1]. החולשה מזריקה קוד זדוני לתהליך לגיטימי של מערכת ההפעלה (לדוגמא explorer.exe) ובכך מצליחה לחמוק מכלי הגנה ולהצפין קבצי מחשב לטובת כופר.

הסקטור הרפואי הוא מטרה מרכזית לתוקפים בתקופה רגישה זו מפאת החשיבות של המשכיות עסקית של גורמי הרפואה מה שיעלה את הסבירות לתשלום דמי הכופר.[2]

[1] https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus
[2] https://www.bleepingcomputer.com/news/security/netwalker-ransomware-infecting-users-via-coronavirus-phishing/

31 Rothschild Blvd.Tel Aviv, 6578414
Office: +972-3-6444417 | info@konfidas.com | www.konfidas.com

#2

כך תוכלו לדעת אילו שמועות נכונות בקשר לקורונה

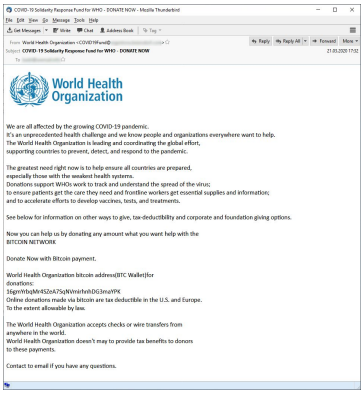
"לא רלוונטי" היא פלטפורמה בה חנן כהן מגיב על מכתבי שרשרת ושמועות דואר אלקטרוני ומקטלג האם רלוונטי או לא. אם אתם לא בטוחים ששמועה מסוימת היא אכן נכונה, תנסו את מזלכם ותבדקו האם ישנה תגובה רלוונטית באתר.

#3

היזהרו, פייק ניוז נוסף מופץ ברשת.

תוכן הודעת הפייק ניוז הוא צו הסגר בירושלים אשר "חתום" על ידי יונה אפשטיין, מנהל אגף הביטחון בדרום והמחוז. יש לשים לב ולהיזהר מהודעות כוזבות רבות, אשר מופצות במדיה החברתית ובערוצים אחרים, ולהקפיד להתעדכן באמצעות ערוצים אמינים, כגון אתר משרד הבריאות וערוץ הטלגרם שלו, פורטל החירום הלאומי של פיקוד העורף והאתר של מערך הסייבר הלאומי.[3]

#4



קמפיין פישינג מתחזה לארגון הבריאות העולמי (WHO)

יחידת המחקר של X-Force זיהתה כמות גדולה של מיילים אשר מגיעים ממקורות שונים אך בעלי אותו שם host - "covid19fund". הקמפיין מתחזה לארגון התורם לארגון הבריאות העולמי (WHO) באמצעות העברת ביטקוין. שימו לב שניתן לתרום כסף ל-WHO באתר הרשמי של הארגון, אך לא באמצעות ביטקוין.[4]

#5

דו"ח של RiskIQ חושף יותר מ-160,000 מיילים מסוג ספאם

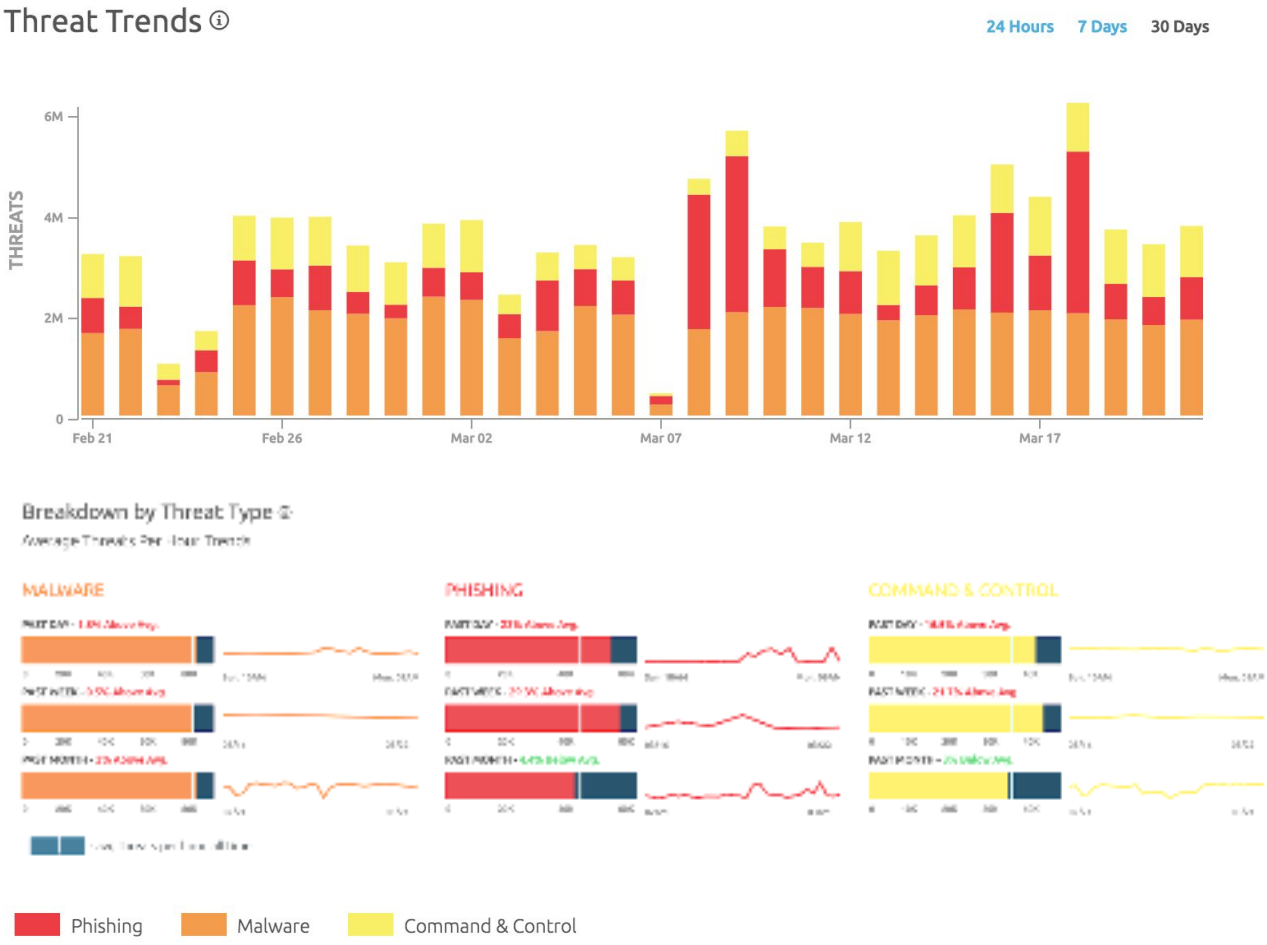
מיילים אלו מכילים את המילים "corona" או "covid" בשורת הכותרת (עדכני לתאריכים 21-22.3). ממצא מעניין נוסף המוצג בדוח הוא הכותרות הנפוצות ביותר של מיילים, ביניהם: "The Mask that can prevent Coronavirus now" - אשר הופיעה ב-13,334 מיילים, "COVID-19 Solidarity Response Fund for WHO - DONATE NOW" שהופיעה ב-9572 מיילים.[5]

[3] https://t.me/MOHreport/3374
[4] https://exchange.xforce.ibmcloud.com/collection/WHO-Coronavirus-Donation-Scam-06813799775b07801e8c26e2dd173de4
[5] https://cdn.riskiq.com/wp-content/uploads/2020/03/COVID-19-Daily-Update-RiskIQ-i3_22-03-2020.pdf

#6

Akamai: עלייה ניכרת בתקיפות הסייבר בחודש האחרון

בהתאמה לדיווחים על קמפיינים רבים הקשורים לקורונה ניתן לראות עלייה משמעותית בשיעור מתקפות הסייבר השונות במהלך החודש האחרון. לדוגמה, באמצע פברואר התבצעו כ-700,000 מתקפות פישינג בעוד שבאמצע מרץ כבר הצטברו כ-3,000,000.[6]



#7

קמפיין סייבר כנגד הסקטור הציבורי במונגוליה מתגלה כאיום עולמי

חוקרי Checkpoint מצאו קשר בין המתקפה במונגוליה למתקפות קשורות באוקראינה, רוסיה ובלארוס. מקור התקיפה הוא בקבצי RTF (סוג קובץ שפותח על ידי חב' מיקרוסופט) אשר הוטמע בהם כלי תקיפה בשם RoyalRoad אשר מנצל

[6] https://www.akamai.com/uk/en/resources/visualizing-akamai/enterprise-threat-monitor.jsp

חולשה ב-Microsoft Word. מבין הפעולות המתבצעות כאשר מריצים קובץ כזה: צילומי מסך של העמדה, יצירת העתק של כלל הקבצים על המחשב, מחיקה ושינוי מיקום קבצים ועוד. ניתן למצוא אינדיקטורים (IOCs) בלינק הזה.[7]

#8

מתקפת כופרה נגד מכון מחקר שעוסק בחיסון לנגיף הקורונה

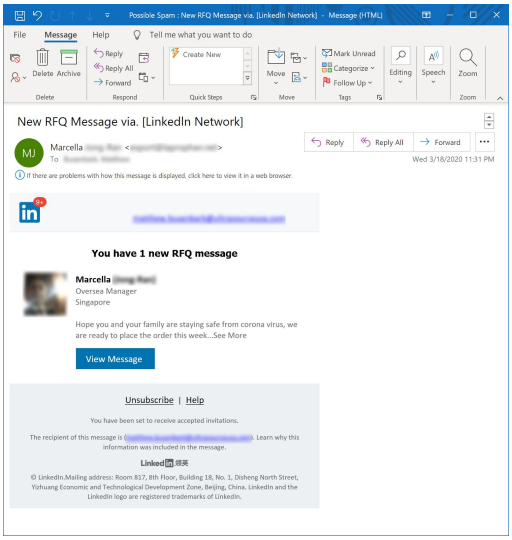
בהמשך למשא ומתן שהתקיים עם קבוצת התקיפה MAZE שחבריה הבטיחו שלא יתקפו מוסדות רפואיים, הקבוצה תקפה את מכון המחקר HMR (Hammersmith Medicines Research) בכופרה. קבוצת התקיפה השיגה נתונים רפואיים אישיים של פציינטים רבים ובתמורה לשמירה על סודיות המסמכים הם דורשים סכום כסף שהמכון לא יכול ולא מוכן לשלם.[8]

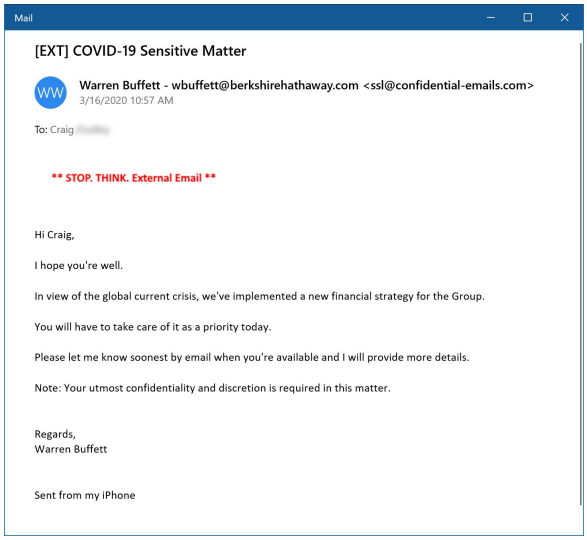
#9

Knowbe4 מציגה דיווחים רבים על מיילים מזויפים

אחד המוצרים של החברה שנקרא Phish alert button מאפשר למשתמשים לדווח באמצעותו על מייל פישינג בו הם נתקלו. ביומיים האחרונים התקלה מסה אדירה של דיווחים מהלקוחות ואכן מרבית המיילים היו מוכרים לפי חקירה שביצעו אצלם, אך התגלו גם מיילים חדשים בזכותה דיווחים.

אריק האווס, חוקר ראשי ב-Knowbe4 מציין[9] כי הוא מעולם לא חזה בתופעה כזו ומציין כי גם אם עד כה היו האקרים שלא ניצלו את בהלת הקורונה, עכשיו מרביתם המוחלט עלו על הגל.[10]

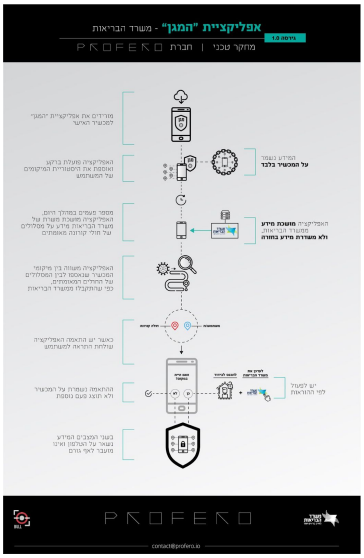




[7] https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
[8] https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus
[9] https://finance.yahoo.com/news/covid-19-phishes-explode-u-120000232.html?.tsrc=fin-srch
[10] https://blog.knowbe4.com/heads-upfeeding-frenzy-covid-19-phishing-attacks-surge-as-u.s.-reels-from-pandemic

סייבר וקורונה בישראל

#10



מומחי סייבר ופרטיות ליווי את תהליך הפיתוח של אפליקציית "המגן"

על פי משרד הבריאות והניתוח של חברת Profero, התקנת האפליקציה היא על בסיס התנדבותי, כאשר איסוף נתוני מיקום בהתבסס על יכולות המכשיר ולא יישלח מידע מהמכשיר של המשתמש. על מנת להבטיח שהאפליקציה כתובה באופן בטוח ואכן שומרת על פרטיות המשתמשים, חברת Profero ביצעה כמהלך מקדים סקירה נרחבת של האפליקציה בדגש על פרטיות ואבטחה על מנת לאשר שהאפליקציה של משרד הבריאות אכן עומדת בעקרונות האלו.

חברת Profero, יחד עם מומחי סייבר נוספים, ימשיכו בבדיקה של כל גרסה חדשה ועדכון שיצא לאפליקציה על מנת להבטיח את המשך השמירה על פרטיות המשתמשים. בתרשים ניתן לראות את אופן פעולת האפליקציה שנבדק ואושר ע"י החברה.[11] הקוד פתוח לקהל הרחב.[12]

#11

הוחלט לא לדחות את שעון הקיץ בשל חסמים טכנולוגיים

בישיבה שהתקיימה הבוקר בראשות המשנה לר׳ המל"ל, הוחלט שלא לדחות את שעון הקיץ לתחילת מאי כיוון שיש מספר היבטים טכנולוגיים אשר עלולים להיפגע מהחלטה זו. תאריך המעבר מוגדר באופן מובנה במערכות ההפעלה של שרתים, מחשבים, ציוד תקשורת ופלאפונים סלולריים ושינוי תאריך ההחלפה יחייב הפצת גרסת תיקון למערכת ההפעלה, לעדכן כל שרת ומחשב ממשלתי ושל גורמים מהותיים רבים במשק.[13]

#12

קרן גלילות קפיטל ממשיכה להשקיע באגרסיביות בסייבר למרות המשבר

בפוסט שהעלה קובי סמבורסקי הוא כותב "אלה לא ימים קלים לכולנו.... קשה לדעת איך יראו הרבעונים הקרובים, דבר אחד בטוח, חדשנות תנצח, סטארטאפים ישראליים ימשיכו להוביל בכל התחומים. אנחנו בגלילות ממשיכים להשקיע באגרסיביות, וממשיכים להאמין ביזמים ישראליים. אם את/אתה מתלבטים, זה בדיוק הזמן להתחיל חברות חדשות![14]

[11] https://www.facebook.com/ProferoSec/photos/a.352381455688065/536289670630575/?type=3&theater
[12] https://github.com/MohGovIL/hamagen-react-native
[13] https://www.gov.il/he/departments/news/news-23-03-2020
[14] https://www.facebook.com/679197661/posts/10158354207662662/?d=n

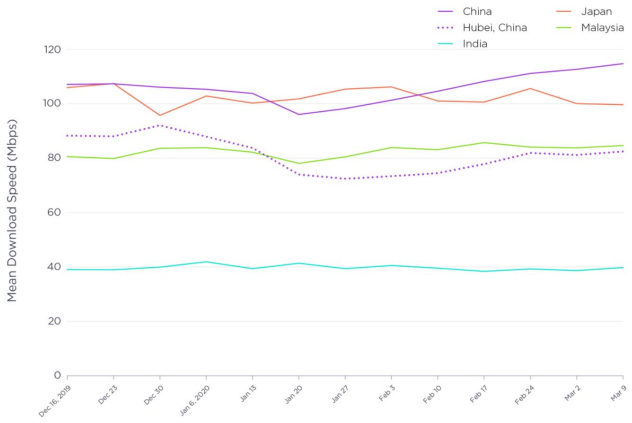
סייבר וקורונה בעולם

#13

Speedtest מציגה את השפעות התפרצות הקורונה על ביצועי האינטרנט

Speedtest מציגה את ההשפעה של הקורונה על ביצועי האינטרנט מבחינת ביצועי רוחב הפס, מהירות הורדת מידע וביצועים ברשת סלולרית ברחבי העולם, בהתמקדות על תמונת המצב בסין בהתמקדות במחוז חובייי עקב ההתפשטות הניכרת.

ניתן לראות כי בשיא התפרצות הנגיף בסין הייתה ירידה דרסטית ברוחב הפס - כלומר במהירות ההורדה של המידע.[15]



#14

מיקרוסופט פועלת למען הגנה מיטבית על לקוחותיה בפני הונאות הקורונה

מיקרוסופט פותחת בנתון, 91% מכלל מתקפות הסייבר מתחילות בהודעת מייל. על כן מיקרוסופט ממקדת מאמצים רבים באיתור וחסימת המיילים הזדוניים השונים, כחלק ממנגנוני ההגנה יש יכולות Machine Learning, חקירה בסביבה מבודלת (בדומה ל-sandbox) וחסימה מהירה של אותו מייל או קובץ.[16]

#15

למרות המשבר העולמי, יש להפקיד על כללי ההגנה על המידע האישי הקבועים ב-GPDR.

ה-European Data Protection Board פרסמה הצהרה בנוגע להגנה על מידע אישי בהתאם ל-GDPR בהקשר התמודדות עם נגיף הקורונה. הצהרת ה- EDPB מתייחסת לכך שהרגולציה האירופית בנושא הגנת המידע האישי, ה-General Data Protection Regulation אמנם מאפשרת עיבוד מידע שנעשה על בסיס לגיטימי לצורך מזעור הנזק

[15] https://www.speedtest.net/insights/blog/tracking-covid-19-impact-global-internet-performance/
[16] https://www.microsoft.com/security/blog/2020/03/20/protecting-against-coronavirus-themed-phishing-attacks/

שנגרם מהמגיפה לכלל העולם, אבל יש עדיין צורך לשמור על שלטון החוק באופן כללי, והמסגרת החוקית לעיבוד מידע אישי והגנת זכויות הפרט בהקשר זה, בפרט. הצהרה לגבי היבטים של הגנת מידע אישי במסגרת ההתמודדות עם התפשטות נגיף הקורונה, הדורשת אמצעי פיקוח שמחייבים עיבוד מידע אישי רב. EDPB מבקש להדגיש כי גם בזמנים חריגים אלה, על ה-Controller ו-Processor להבטיח את ההגנה על המידע האישי של נושאי המידע. הקביעה של מצבי חירום מאפשרת בסיס חוקי לעיבוד מידע העלול לתת לגיטימציה לפגיעה בחירויות; וחיוני להבטיח שכל מגבלה על הגנת מידע אישי היא מידתית ומוגבלת לתקופת החירום.[17]

#16

שיתוף פעולה של ממשלת ארה"ב עם מספר חברות לצורך חקר נגיף הקורונה

מבין החברות התורמות משאבי מחשוב: IBM, Google, Microsoft, ו-Amazon. החברות יתרמו גישה למשאבי מחשוב עם מהירות עיבוד גבוהה, לצורך זירוז הניתוח של כמות מאסיבית של מידע וממצאים - ניתוח שיסייע במאמצים הרפואיים והמדעים למגר את נגיף הקורונה.[18]

#17

משרד המשפטים בארה"ב נוקט בפעולות אכיפה נגד הונאות שקשורות למגיפת COVID-19

היום נפתח התיק הראשון כנגד מפעיל אתר מזויף (coronavirusmedicalkit.com), אשר הציעה לגולשים ערכות חיסון מזויפות תמורת תשלום ומסירת פרטי כרטיס אשראי. בשלב הראשון, המשרד מוציא צו סגירה של האתר והצהרה כי יינקטו בכל פעולה אפשרית על מנת למגר את תופעת ההונאות האינטרנטיות בעקבות נגיף הקורונה.[19]

#18

132 ארגונים ברחבי ארה"ב פרסמו הצהרה משותפת בבקשת שקיפות של הממשלה בנוגע להתמודדות עם הנגיף

בזמנים רגישים אלו, שוררת בהלה ופחד בכל העולם עקב אי-וודאות בנוגע להתפשטות נגיף הקורונה. אותם 132 הארגונים מפצירים בממשלת ארה"ב שלא תערוך פגישות וקבלת החלטות בנושא הקורונה בסודיות, אלא שהיא תאמץ מדיניות של שקיפות על מנת לצמצם את אי-הוודאות. בנוסף, בהצהרה מעודדים את הממשלה להנגיש את כלל המידע לאזרחים באמצעות פלטפורמות טכנולוגיות.[20]

#19

ממשלת קנדה מורידה אתרים מזויפים הקשורים לנגיף הקורונה

[17] https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf
[18] https://techcrunch.com/2020/03/22/ibm-amazon-google-and-microsoft-partner-with-white-house-to-provide-compute-resources-for-covid-19-research/
[19] https://www.justice.gov/opa/pr/justice-department-files-its-first-enforcement-action-against-covid-19-fraud
[20] https://www.nfoic.org/sites/default/files/2020-03/132%20Organizations%20Sign%20Statement%20on%20Government%20Coronavirus%20Emergency%20Transparency%20and%20Access%20March%2020,%202020.pdf

המרכז הלאומי לסייבר בקנדה מוריד אתרים המתחזים לרשויות בריאות ולאתרים ממשלתיים של קנדה. דוגמה למקרה הונאה שדווח הוא שליחת הודעות מזויפות לאזרחים, בהן נאמר כי הם נדבקו בנגיף ועל מנת לקבל תרופות הם צריכים להעביר את פרטי האשראי שלהם.[21]

#20

הסוכנות הפדרלית לניהול מצבי חירום (FEMA) הקימה עמוד לניהול שמועות בנושא הקורונה

עקב הודעות פייק ניוז מרובות, FEMA פתחו עמוד באתר הרשות שמרכז את כלל השמועות והמיתוסים בנוגע להתפשטות נגיף הקורונה. בין היתר, מטרת העמוד היא לצמצם את בהלת האזרחים, שלילת מידע כוזב, והצגת עובדות מדעיות ובדוקות.[22]

פתרונות

#21

שני טיפים של חב' Fire Eye לעבודה מרחוק מאובטחת ככל הניתן

המשק הישראלי מתחיל להתרגל לעבודה מהבית (teleworking) ועושה שימוש בפרוטוקולי תקשורת להתחברות מרוחקת נפוצים אך בחיבור ישיר למערכות קריטיות: תופעה שיוצרת באופן מיידי סיכון גבוהה להשגת גישה לאותן מערכות קריטיות. שתי המלצות להורדת הסיכון הינן (1) להטמיע Multifactor Authentication בגישה למערכות, ו-(2) הטמעת אנטי-וירוס על כלל העמדות המרוחקות ללא יוצא מן. [23]

#22

מיקרוסופט מפרסמת כלי לניהול תקשורת בזמן משבר

חב' מיקרוסופט משחררת גרסה ראשונה של כלי חדש, Crisis Communication, שמטרתו לעזור בתיאום ושיתוף מידע בין צוותי תגובה בזמן משבר כמו משבר הקורונה. הפתרון מיועד ליישום מהיר של כל ארגון לקוחות ומאות ארגונים כבר משתמשים בו.[24]

#23

הנחיות של איגוד הטלקום הבינלאומי (ה-ITU) למדינות בהספקת תקשורת חירום בזמן נגיף הקורונה

[21] https://www.cbc.ca/news/politics/cse-disinformation-spoofing-1.5504619
[22] https://www.fema.gov/coronavirus-rumor-control
[23] https://www.fireeye.com/blog/executive-perspective/2020/03/remote-work-in-an-age-of-covid-19-threat-modeling-the-risks.html
[24] https://powerapps.microsoft.com/en-us/blog/crisis-communication-a-power-platform-template/

איגוד הטלקום העולמי (International Telecommunication Union) פרסם הנחיות שתומכות בשרידות מערכות תקשורת לאומיות ובינלאומיות במצבי חירום. המזכ"ל הולין ז'או מדגיש את החיוניות של מערכות תקשורת כעת, כחלק מהתמודדות עם התפשטות הקורונה וכדי לאפשר ניהול אירועים ומצבי חירום. האיגוד כבר מסייעת למספר מדינות בבניית תוכניות לאומיות לתקשורת חירום.[25]

הציטוט היומי

"כשתמודדים עם משהו כמו התקפת מניעת שירות [DDoS] על מחלקת בריאות ושירותי אדם [HHS, משרד הבריאות בארה"ב] בזמן מגיפה, זו פעולה חמורה שמדינה אחרת יכולה לנקוט. אז אם זו אכן מדינה אחרת שמבצעת פעולה כזאת, בטוחני שההשלכות תהינה קשות."[26]

ויליאם בר,

התובע הכללי האמריקאי

(בהתיחסות למתקפת DDOS על מוסדות בריאות בארה"ב[27])

לעדכונים נוספים

ערוץ הטלגרם: https://t.me/corona_cyber_news

טוויטר: https://twitter.com/konfidas

פייסבוק: https://www.facebook.com/konfidas

אתר האינטרנט של קונפידס: https://www.konfidas.com/

הבלוג של קונפידס: https://medium.com/konfidas

*** סוף המסמך ***

[25] https://www.itu.int/en/mediacentre/Pages/PR05-2020-new-guidelines-for-national-emergency-telecommunication-plans.aspx

[26] https://www.washingtonpost.com/opinions/2020/03/19/this-is-not-time-leave-our-hospitals-unprotected-against-cyberattacks/

[27] https://abcnews.go.com/Health/facing-coronavirus-pandemic-us-confronts-cyber-attacks/story?id=69653329