חדשות סייבר ונגיף הקורונה (COVID-19)

עדכון יומי ליום ב', 30.03.2020

הדוח מתפרסם גם במדור
"קפטן אינטרנט" של עיתון הארץ

הדוח מתפרסם גם בסייברנט

עיקרי הדברים

1. מתקפת סייבר מזהירה על שהות, לכאורה, בקרבת חולי קורונה ובפועל מדביקה בתוכנה זדונית.
2. מערך הסייבר הלאומי מפרסם קול קורא ליצירת Marketplace לסייבר.
3. Check Point: פושעי סייבר מטרגטים את חברת Zoom בשל הפופולריות שלה.
4. חברות בעולם רוכשות תוכנות מעקב אחר עובדיהן כדי לפקח על תפוקתם.
5. הסייבר במקום הגבוה ביותר באתר ארגון הבריאות העולמי.

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

תוכן עניינים

איומים, התקפות והתראות

פייק ניוז מטעם משרד הבריאות

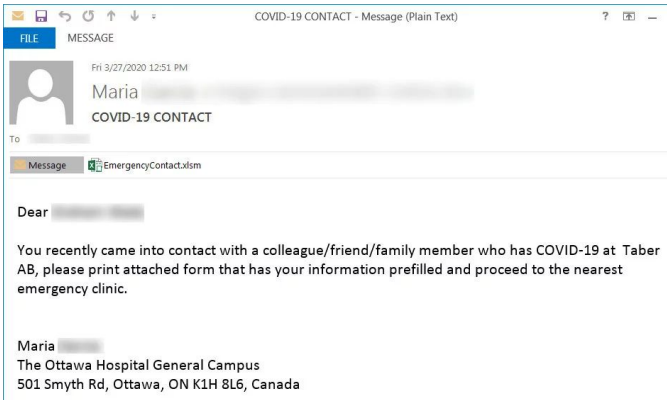
משרד הבריאות דיווח על הודעה מזויפת בה נמסר כי מנכ"ל משרד הבריאות אובחן כחולה בקורונה, וכי מתבצעים דיונים על מקום אשפוזו על מנת שיוכל להמשיך בעבודתו. חשוב לעקוב אחר הערוצים של משרד הבריאות על מנת לקבל מידע אמין והתראות על מידע כוזב (אתר משרד הבריאות, ערוץ הטלגרם של משרד הבריאות).[1]

פייק ניוז - SMS בגין קנס בעקבות עבירות על הנחיות משרד הבריאות

ברשתות החברתיות ובוואטספ מופצת תמונה של הודעת SMS מזויפת, לכאורה ממשרד הבריאות, המודיעה למשתמש על קבלת קנס לאור הפרת הנחיית המשרד להישאר ברדיוס 100 מטרים ממקום המגורים.

מתקפת סייבר המבוססת על אזהרה כוזבת בדבר שהות בקרבת חולי קורונה

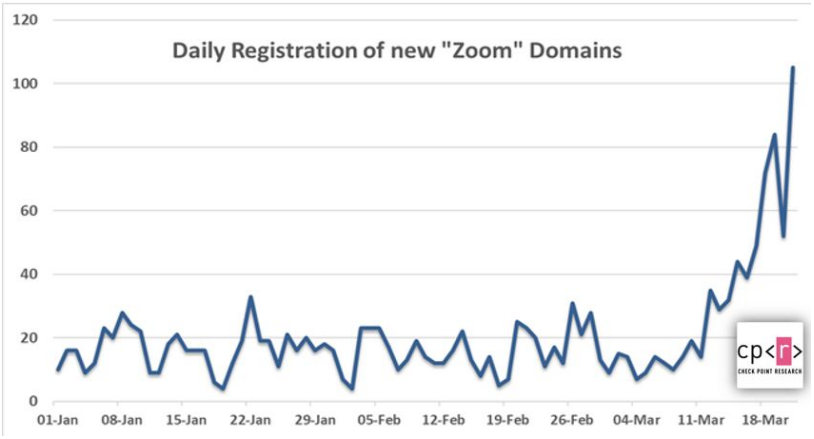
בקמפיין זה נשלחות הודעות אימייל מזויפות שמקורן לכאורה בבית חולים מקומי. ההודעות פונות לקורבנות בטענה כי היו ליד חולה קורונה מאומת וכי עליהם להוריד קובץ מצורף המכיל את הקליניקות הקרובות ביותר שאליהן ניתן לגשת לצורך בדיקה. בעת פתיחת הקובץ המצורף תרוץ נוזקה אשר מזריקה קטעי קוד זדוניים לתהליכים לגיטימיים של מערכת ההפעלה Windows, שמטרתם לגנוב מידע, בדגש על ארנקים קריפטוגרפיים ו- cookies.[2]



[1] https://t.me/MOHreport/3531
[2] https://www.bleepingcomputer.com/news/security/phishing-attack-says-youre-exposed-to-coronavirus-spreads-malware/

Check Point: פושעי סייבר מנצלים את הפופולאריות של פלטפורמות לקיום פגישות מרחוק

בשל התפרצות וירוס קורונה ישנה עליה בפופולריות בתוכנות תקשורת מרחוק, כאשר הפופולארית ביניהן היא פלטפורמת Zoom. לפי Check Point ישנה עליה ברישום הדומיינים המזויפים ותוכנות זדוניות המכילים את המילה Zoom ובאתרי פישינג המזכירים פלטפורמות מובילות אחרות דוגמת Classrom של גוגל.[3]



פישינג מטעם ראש ממשלת סינגפור עם פניה אישית לבקשת סיוע

לי הסיין לונג, ראש ממשלת סינגפור, הזהיר היום מפני קמפיין פישינג המתבסס על הודעה בטוויטר, לכאורה מטעמו. הוא מבקש שלא להשיב עליה ובהחלט לא לספק מבקשים מידע אישי.[4]

הטרנדים האחרונים במתקפות הפישינג

דוח מתעדכן של PhishLabs מציג סוגים שונים של מתקפות פישינג הקשורות לנגיף הקורונה. הקטגוריות שמוצגות בעדכון האחרון הן: גניבת פרטי התחברות לחשבון מייל, הונאות המבוססות על דרישות תשלום מהקורבן והונאות באמצעות התחזות לעמותות צדקה. בדוגמה הבאה ניתן לראות מייל מזויף מ"מרכז הבריאות הלאומי"(national health center), שטוען כי מצורפת אליו רשימה של חולי קורונה חדשים באזור המגורים של הנמען. בפועל, כאשר המשתמש מקיש על הלינק, הוא מועבר לעמוד התחברות למייל, ובכך התוקף גונב את פרטי ההתחברות שלו.[5]


From: CDC <nationalhealthcenter@gravitt.net>
Sent on: Wednesday, February 12, 2020 6:40:27 PM
To: [redacted]
Subject: CDC Health Alert: COVID-19 Emergency [EXTERNAL]

Distributed via the CDC Health Alert Network
February 13, 2020
CDCHAN-00426

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

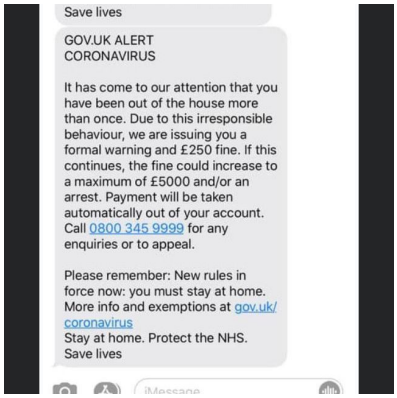
You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing

[3] https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/; https://thehackernews.com/2020/03/zoom-video-coronavirus.html

[4] https://twitter.com/leehsienloong/status/1244458978987237376?s=20

[5] https://info.phishlabs.com/blog/covid-19-phishing-update-threat-actors-target-cdc-who



פייק ניוז מטעם ממשלת בריטניה על תשלום קנס בגין הפרת בידוד

הודעה מזויפת מטעם ממשלת בריטניה קובעת, כי על מקבל ההודעה יש לשלם קנס של 250 פאונד על כך שהפר בידוד. עוד נטען כי אם לא ישלם, הקנס צפוי לעלות ל-5,000 פאונד. על פי ההודעה, התשלום על הקנס מתבצע באופן אוטומטי והיא מכילה מספר טלפון לצורך פניה ובירורים. המספר מוביל, ככל הנראה, לעבריינים שגובים כסף בשם המשטרה, לכאורה, או סוחטים את הקורבן. גם בארץ נשלחו מספר הודעות פייק ניוז בעלות תוכן דומה.[6]

פוגען לתקיפות גופים פיננסיים מוסב לגניבת מידע בהקשר הקורונה

פוגען Zeus, אשר התגלה כבר בשנת 2015 ומכוון לסקטור הפיננסי, חוזר להופיע בקמפייני פישינג על בסיס הודעות מייל, אשר מכילות צרופה בשם COVID 19 relief מסוג doc//.docx. בפתיחתה מורד למחשב הנתקף קובץ בעל יכולות כתיבה לקבצים על גבי מערכת ההפעלה והאזנה למידע על גבי המחשב. המידע אותו אוסף הכלי הינו לרוב פיננסי, משום שקונפיגורציית הכלי - שבעבר שימש לתקיפת בנקים בארה"ב, קנדה, ואוסטרליה - לא שונתה.[7]

קמפיינים של פישינג בסקטור המשפטים, הפארמה, הנדסת התוכנה ועוד

צוות המחקר של IBM פרסם בבלוג שלו דיווח על מחקר של המוסד למחקר חדשנות ומדע, Institute for Research on Innovation and Science (IRIS). חוקרי IRIS זיהו מספר קמפייני פישינג ממוקדים ברחבי העולם, אשר מכוונים, בין היתר, למשרדי עורכי דין בין לאומיים באירלנד, לתעשיית הנדסת התוכנה באוקראינה, לתעשיית הפארמה בגרמניה, באיטליה ובצרפת ועוד. על פי הדיווח נעשה שימוש מוגבר בנוזקות מוכרות, כגון JS Cryxos Trojan, Hawkeye, Netwalker, Kryptik ועוד. לפי הנתונים שבידם לא מזוהה ירידה במספר התקיפות העוסקות בנגיף הקורונה.[8]

[6] https://coronavirusphishing.com/2020/03/30/text-gov-uk-alert/

[7] https://securityintelligence.com/posts/zeus-sphinx-trojan-awakens-amidst-coronavirus-spam-frenzy/

[8] https://exchange.xforce.ibmcloud.com/collection/Threat-Actors-Capitalizing-on-COVID-19-f812020e3eddbd09a0294969721643fe

סייבר וקורונה בישראל

מערך הסייבר הלאומי מפרסם קול קורא ליצירת Marketplace לסייבר

בעקבות המעבר של ארגונים רבים לעבודה מרחוק, פרסם מערך הסייבר הישראלי קול קורא המעודד חברות להשתתף ב"זירת מפגש" (Marketplace) בין המשק לבין מוצרים ושירותים בתחום הסייבר. היוזמה לשעת חירום תאפשר לארגונים וליחידים להציג מוצרים ושירותים בתחום הגנת הסייבר, שמותאמים לאיומים ולסיכונים הנובעים מהשלכות הקורונה על רמת החוסן של המשק הישראלי.[9]

משרד הבריאות מודיע על העברת פרטי חולי הקורונה והמבודדים לכלל הרשויות הישראליות

משרד הבריאות פרסם בערוץ הטלגרם המיועד לענייני הקורונה את כוונתו להעביר את המידע על החולים והמבודדים לכלל הרשויות, תוך שמירה על חיסיון מידע וצנעת הפרט, במטרה "לאפשר לרשויות ליישם את תפקידיהן בסיוע במציאת פתרונות למבודדי בית בתחומן שלא יכולים לקיים את תנאי הבידוד בביתם, איתור אנשים שנחשפו לחולים שלא ניתן להגיע אליהם בדרך אחרת והושטת סיוע לחולים ולמבודדים הזקוקים לסיוע".[10]

משטרת ישראל פתחה ב-40 חקירות נוספות בעקבות חשד להפצת פייק ניוז [11]

מתחילת משבר הקורונה ועד כה נפתחו 152 חקירות בנושא הפצת ידיעות כזב.

משרד המשפטים והרשות להגנת הפרטיות פרסמו המלצות הנוגעות לשימוש ברחפנים

משרד המשפטים והרשות להגנת הפרטיות פרסמו אתמול מסמך, בו הם מתייחסים לסוגיית השימוש הגדל ברחפנים בשטח הארץ, הדינים המחייבים בהיבטי הפרטיות והאופן שבו יש להתייחס למידע אשר נאגר בתוך הרחפן. הרשות מפרטת את המלצותיה לגבי היבטי הפרטיות בשימוש ברחפנים, שבליבן עקרון מנחה של מידתיות: "להפעיל את הרחפן באופן מידתי, שיצמצם למינימום ההכרחי את היקף המידע האישי הנאסף, או את המשך העיבוד שלו אם נאסף, בדגש על מידע רגיש בעל פוטנציאל גבוה להשפיע על פרטיות המצולמים. מתכונת הפעלת הרחפן צריכה להיקבע באופן ספציפי, לפי חשיבות מטרת האיסוף ולאחר ביצוע תסקיר השפעה על פרטיות". [12]

הפיקוח על הבנקים הודיע על הקלות בצירוף לקוחות לביצוע פעולות מרחוק

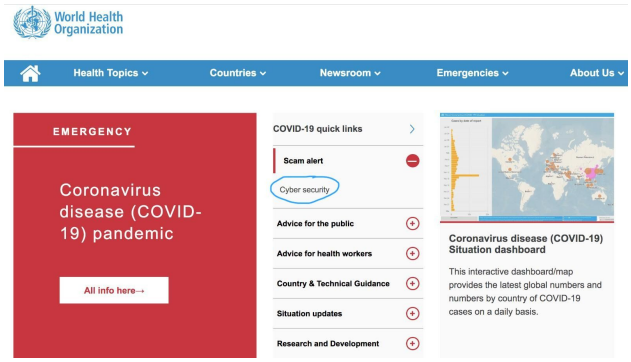
עקב הנחיות משרד הבריאות וצמצום שירותי קבלת הקהל בסניפי הבנקים, הפיקוח על הבנקים מעודד אותם להנפיק ללקוחותיהם כרטיסי חיוב מיידי (דביט), אשר באמצעותם ניתן לבצע משיכת מזומן וביצוע עסקאות רכישה בין אם בבתי העסק ובין אם מרחוק. על הבנקים לאתר את הלקוחות שאין להם כרטיסי אשראי או חיוב ולהזמינם להצטרף לשירות.[13]

[9] https://www.gov.il/he/departments/publications/Call_for_bids/cmarket
[10] https://t.me/MOHreport/3533
[11] https://www.gov.il/he/departments/news/police_covid-19_information_general
[12] https://www.gov.il/he/departments/publications/reports/drone_recommendations
[13] https://www.boi.org.il/he/NewsAndPublications/PressReleases/Pages/30-3-2020.aspx

הרשות להגנת הפרטיות פרסמה הנחיות בנושא חתימה אלקטרונית בעקבות הקורונה

בעקבות התפרצות נגיף הקורונה והמעבר לשימוש מוגבר בשירותים דיגיטליים, הרשות להגנת הפרטיות מפרסמת שתי הנחיות שמטרתן להתאים את הדרישות בעת תהליך הנפקת תעודות אלקטרוניות מאושרות. ההנחיה הראשונה מפרטת את האופן בו הגורם המאשר צריך לפעול לשם קיום הוראות חוק החתימה האלקטרונית. ההנחיה השנייה עוסקת בתהליך ביצוע חידוש (מרחוק) לתעודה אלקטרונית מאושרת שטרם פג תוקפה.[14]

סייבר וקורונה בעולם



הסייבר ראשון באתר ארגון הבריאות העולמי

העליה החדה של מתקפות הסייבר מחודש ינואר שמה את נושא מתקפות הסייבר ב-quick links שבראש עמוד אתר הבית של ארגון הבריאות העולמי (WHO). התייחסות הארגון כוללת אזהרה מפני התחזות של פושעי סייבר לארגון עצמו, ואת הצהרתו, לפיה לעולם לא יבקש פרטים אישיים מיחידים.[15]

חברות בעולם רוכשות תוכנות מעקב אחר עובדיהן כדי לפקח על תפוקתם

באתר Bloomberg התפרסם כי חברות רבות רוכשות תוכנות שמטרתן לעקוב אחר ההתנהלות של בעלי המחשבים עליהם היא מותקנת. תוכנות אלה מסוגלות לקלוט הקשות מקלדת, לבצע תצלומי מסך ולעקוב אחר ההדפסות היוצאות. מנכ"ל אחת החברות מציין כי "זוהי הזדמנות של העובדים להוכיח למנהלים שלהם שהם יכולים לסמוך עליהם."[16]

מחקר של חברת Shodan חושף עלייה משמעותית בשימוש בפרוטוקול RDP בשימוש חברות וב-VPN בשימוש אישי

מחקר מקיף של חברת Shodan מצביע על עלייה של 41% מאז פרוץ הקורונה בשימוש בפרוטוקול RDP, המשמש חברות לשליטה מרחוק של שרתי/עמדות Windows. מגמה נוספת שעלתה מן המחקר היא עלייה של 33% בשימוש אישי בשירותי VPN בכדי לגשת לתוכן שחסום בארץ בה מתגוררים האנשים.[17]

[14] https://www.gov.il/he/departments/news/electronic_sign_corona
[15] https://www.who.int/
[16] https://www.bloomberg.com/news/features/2020-03-27/bosses-panic-buy-spy-software-to-keep-tabs-on-remote-workers
[17] https://blog.shodan.io/trends-in-internet-exposure/

Zoom מסירה קוד באפליקציית האייפון שהעביר פרטי משתמשים לפייסבוק

במחקר שערכה חברת Motherboard, התגלה כי פרטי משתמשים של אפליקציית Zoom באייפון הועברו לפייסבוק. חוקרי Motherboard ציינו כי העברת האינפורמציה הזו לא צויינה בבירור במדיניות הפרטיות של החברה. בפנייה רשמית לחברת Motherboard, חברת Zoom הודיעה כי הסיבה להעברת המידע היא שימוש במבנה קוד (SDK) של לפייסבוק, אשר שלף מידע לא הכרחי מהאפליקציה לצורך השירות "התחבר באמצעות פייסבוק".[18]

ממשלת בריטניה פועלת לצמצום התפשטות מידע כוזב ברשת

מומחים ברחבי העולם מרחיבים את מאבקם בפייק ניוז בנושא הקורונה. ממשלת בריטניה מזהה כ-70 ידיעות בשבוע הכוללות מידע כוזב ומזוייף. בתגובה לכך, משרדי הממשלה נוקטים בפעולות מחמירות להסרת מידע כוזב באופן יזום מהרשת ומשיקים את קמפיין "Don't Feed The Beast", המציג 5 מאפיינים שיש לבדוק לפני שמשתפים פוסט שעלול להיות פייק ניוז ותורמים להפצת המידע השגוי.[19]

ה-ICO הבריטי מאשר שימוש במידע מטלפונים סלולריים לצורך מעקב אחר התפשטות הנגיף

בהמשך למספר מדינות ברחבי העולם שכבר מפעילות שימוש בנתונים של טלפונים סלולריים לטובת איתור חולי קורונה, גם המשרד להגנת המידע הבריטי מאשר שימוש בנתונים כאלה, לאחר שעברו תהליך אנונימיזציה, ככלי ממשלתי לצמצום התפשטות נגיף הקורונה. ההנחה היא שמכיוון שהמידע נשמר בצורה אנונימית, שלא מקשרת את נשוא המידע למידע עצמו, הם אינם כפופים לכללי רגולציית הגנת מידע.[20]

סוכנות אירופית קובעת כי אין ירידה באיכות הגלישה באינטרנט עקב הקורונה

בהמשך לדוחות רבים, שמציגים ירידה משמעותית באיכות הגלישה עקב הגברת התעבורה בצורה משמעותית, מדווחת הסוכנות האירופאית לרגולציית תקשורת אלקטרונית (BEREC), כי על אף העליה המשמעותית בשימוש ברשתות נתוני הסלולר, לא נחוותה באירופה ירידה משמעותית במהירות הגלישה.[21]

[18] https://www.vice.com/en_us/article/z3b745/zoom-removes-code-that-sends-data-to-facebook
[19] https://www.gov.uk/government/news/government-cracks-down-on-spread-of-false-coronavirus-information-online
[20] https://www.theregister.co.uk/2020/03/29/ico_anonymised_location_data_coronavirus/
[21] https://berec.europa.eu/eng/document_register/subject_matter/berec/press_releases/9238-press-release-berec-report-on-the-status-of-internet-capacity

פתרונות

חברת Indusface מעניקה חודש חינם לשירותי אבטחת מידע שונים לארגונים שנפגעו מהשלכות וירוס הקורונה

אמש הודיעה חברת Indusface על מתן שירותי אבטחת מידע שונים לחברות שספגו פגיעה כתוצאה מווירוס הקורונה למשך חודש ללא עלות. כיום החברה כבר מציעה לכלל הציבור שירות חינם להערכת מצב אבטחת המידע באתר על ידי סריקה חיצונית, ואף מעניקה בחינם למשך חודש את השירותים הבאים: Web Application scanning, CDN, DDoS protection.[22]

ה-ICO הקימה פורטל לצורך ריכוז מידע הנוגע להגנת המידע בעת משבר הקורונה

לצורך הנגשת המידע, ICO הקימה פורטל בו היא מרכזת את כלל השימוש בסוגי המידע האישי הנוגע לקורונה. הפורטל יכיל מידע בנושאים כמו שימוש בטלפון לצורך מעקב אחר חולים, שאלות נפוצות ותשובות ועוד.[23]

העשרה

חברת Cyber 2.0 מכריזה על אתגר ההאקרים השלישי, הנושא פרס בגובה 10,000 ש"ח

לאחר שהשיקה שירותי סייבר בענן ומתן מערכת הגנה לעובדים מהבית, הכריזה חברת Cyber 2.0 על אתגר שלישי, אשר הפעם יתבצע מהבית. אם אף האקר לא יצליח לפרוץ את המערכת החדשה של החברה, תתרום החברה את הפרס הייעודי של 10,000 ש"ח לעמותת "החבר'ה הטובים", המחלקת חבילות מצרכים לנזקקים.[24]

חלל וקורונה

תמונות לוויין הממחישות מה קורה בכדור הארץ כאשר הכל עוצר.[25]

[22] https://thehackernews.com/2020/03/apptrana-web-app-security.html
[23] https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/
[24] https://www.israeldefense.co.il/he/node/42381
[25] https://www.bloomberg.com/features/2020-coronavirus-satellite-photos-before-after/

הציטוט היומי

"התלות שתיווצר בתקשורת מרחוק, תאיץ גם טכנולוגיה אחרת ובלתי צפויה: הטכנולוגיה של לווייני תקשורת. מקצועות המחשבים, החלל ואבטחת הסייבר יהיו ללא ספק דומיננטיים בשוק מקצועות העתיד."[26]

פרופ' יצחק בן ישראל,

יו"ר סוכנות החלל הישראלית

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 ***

[26] https://www.facebook.com/permalink.php?story_fbid=10158131017780818&id=776620817