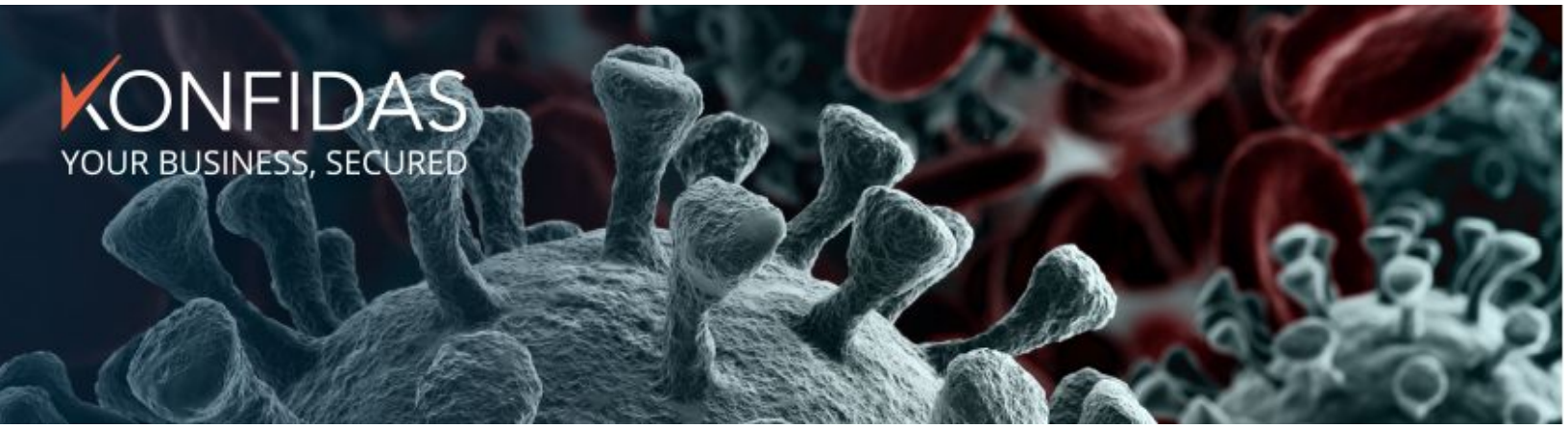


חדשות סייבר ונגיף הקורונה (COVID-19)

עדכון יומי ליום ג', 1.04.2020

הדוח מתפרסם גם במדור
"קפטן אינטרנט" של עיתון הארץ

הדוח מתפרסם גם בסייברנט

עיקרי הדברים

1. חולשה מסוכנת באפליקציית Zoom
2. משרד התקשורת: עליה של 15% בתעבורת האינטרנט בסיבים התת מימיים מישראל ו-25% בתקשורת הנייחת.
3. ממשלת ישראל הוסיפה סעיפים לתקנות שעת חירום המסירים את חובת מחיקת המידע הנאסף לאחר תום המגפה.
4. גוגל סופגת ביקורת קשה על כך שמאפשרת מכירת מסכות וחיסונים מזוייפים כנגד נגיף הקורונה
5. ריכזנו לנוחיותכם את המוצרים והשירותים בתחום הסייבר הניתנים בחינם במהלך תקופת הקורונה.

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

תוכן עניינים

הציטוט היומי

"בנסיבות רגילות 1 באפריל הוא מסורת של גוגל וזמן לחגוג את מה שהופך אותנו לחברה לא שגרתית. השנה אנו הולכים לקחת הפסקה ממסורת זו, מתוך כבוד לכל אלה שנלחמים בנגיף הקורונה המטרה החשובה ביותר שלנו כרגע היא לסייע לאנשים, אז בואו נשמור את הבדיחות לאפריל הבא, שללא ספק יהיה הרבה יותר משמח מהאפריל הזה."[1]

לוריין טוהיל,
מנהלת השיווק הראשית של חב' גוגל

איפה אפשר לקרוא את הדוחות?

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

[1] https://9to5google.com/2020/03/27/google-is-calling-off-april-fools-this-year-according-to-an-internal-email/

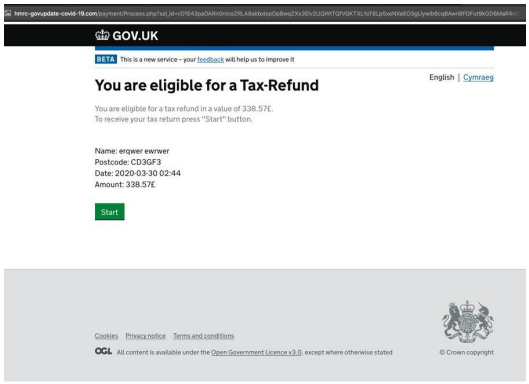
איומים, התקפות והתראות

חולשה מסוכנת באפליקציית Zoom

במהלך השבוע התגלתה חולשת Zero Day מסוג UNC path injection בפלטפורמת Zoom. מדובר בסוג מוכר של חולשה ללא פתרון, שניצולה מאפשר גניבת סיסמאות ממחשבים. החולשה מאפשרת לשלוח בצ'אט של שיחת ועידה גם נתיב לתיקיה כקישור לחיץ (ולא רק קישורים לכתובות URL). לחיצה על קישור לניתוב תשתף עם התוקף את שם המשתמש והסיסמא. שליחת לינק זדוני מסוג זה בצ'אט של שיחת ועידה מאפשרת חדירה למחשבים של כלל משתתפי השיחה. **כדי להימנע ממתקפה מסוג זה מומלץ לא ללחוץ על אף לינק בצ'אט.** כמו כן, נזכיר כי בנוסף לאיום הנ"ל, דיווחנו בדוחות האחרונים על מתקפות נוספות הקשורות לפלטפורמת Zoom, מסוג "Zoombomming". על פי נתונים של Apple App store, אפליקציית זום הותקנה במהלך השבוע 2.13 מיליון פעמים. העלייה החדה בשימוש באפליקציה הפכה אותה לפופולריות במיוחד גם בקרב ההאקרים, רבים מהם מציגים תמונות אנטישמיות בשיחות זום לא מאובטחות, ואף חודרים לשיחות ועידה בבתי ספר.[32]

קמפיינים של התחזות לגופים פיננסים מדיניים באנגליה וצרפת לגניבת פרטי אשראי

הקמפיין הראשון מתחזה לגוף במשרד הכלכלה בצרפת, מינהל המימון הציבורי (Direction générale des finances publiques), אשר אחראי על מתן תמיכה כלכלית לעסקים קטנים ועצמאיים, עקב ההשלכות הכלכליות של נגיף הקורונה על המשק. האתר המזויף מבקש מהקורבנות להזין את שם, כתובת, ופרטי האשראי שלהם. על כתובת המקור ממנה יצא הקמפיין נמצאו כתובות פישינג נוספות, המתחזות ל-Paypal.[4] קמפיין נוסף מתחזה לשירות beta שניתן על ידי גוף מדיני באנגליה, ה-HMRC, שגם הוא אחראי למתן סיוע פיננסי למי שנפגע כלכלית מנגיף הקורונה. בדומה לקמפיין באתר הצרפתי, באתר ה-HMRC, קורבנות מזינים שם ופרטי אשראי.[5]



מתקפות כופרה, מפות קורונה מזויפות ועשרות מתקפות פישינג בצל הקורונה

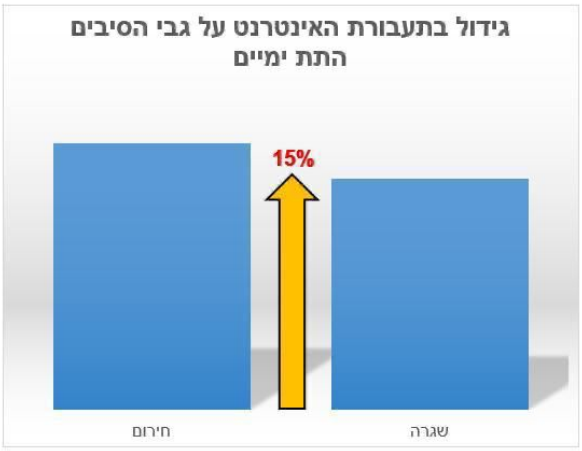
התקיפות אשר מוצגות בדו"ח מייצגות דוגמאות נפוצות ממספר רב של מתקפות, כגון מפות מזויפות למעקב אחר הקורונה, מתקפת הכופרה CovidLock, ומתקפות פישינג רבות על גבי אתרים ואפליקציות. כדי להימנע מתקיפות, חברת קונפידס מציעה שישה צעדים פשוטים להגנה: יש להיכנס רק לאתרים רשמיים ואמינים, להתקין אפליקציות מחנויות אפליקציות בטוחות כמו App Store, Google Play ו- Microsoft, לעדכן גרסאות תוכנה בתכיפות, לא לפתוח דבוקות דואר

[2] https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-via-unc-links/
[3] https://www.haaretz.com/us-news/zoombombing-anti-semitic-hackers-target-jews-during-online-meetings-on-zoom-1.8730709
[4] https://www.securitymagazine.com/articles/92026-two-new-covid-19-related-phishing-scams
[5] https://twitter.com/PhishingAi/status/1244738961446178823

אלקטרוני ממקור לא מוכר, לא לאפשר לאפליקציות או תוכנות הרשאות יתר, ולהשתמש באנטי-וירוסים עדכניים על המכשירים הסלולריים.[6]

סייבר וקורונה בישראל

משרד התקשורת: עליה של 15% בתעבורת האינטרנט בסיבים התת מימיים מישראל ו-25% בתקשורת הנייחת



חל גידול גידול משמעותי בתעבורת הנתונים בתקשורת הנייחת (כ- 25% בממוצע יומי), הגורם לעומסים והאטה בשעות השיא; עם זאת, ללא חריגה מהנורמה מפרוץ המשבר. כמו כן, נרשם גידול בכמות השיחות הסלולריות בכ- 25%-20% מהממוצע בשגרה, אך ללא חריגה מהנורמה בזמן המשבר.

רשתות התקשורת פועלות באופן תקין למרות העומסים הגבוהים מהרגיל בהשוואה לתקופת שגרה. לא דווחו אירועים חריגים ברשתות הסלולר, בטלפונים הנייחים וקווי ואינטרנט.

היום דווח על כ-3500 ניודים בין החברות, לעומת מעל 8000 בשגרה.[7]

ממשלת ישראל הוסיפה סעיפים לתקנות שעת חירום, המסירים את חובת מחיקת המידע הנאסף לאחר תום המגפה

ממשלת ישראל הוסיפה לתקנות שעת חירום התש"ף -2020 שני תיקוני תקנות, אשר פוטרות מרשויות השלטון השונות את הצורך למחוק את המידע אשר נאסף במהלך זמן מגפת הקורונה, עד אשר שתיקבע החלטת הממשלה בנושא.[8]

עמותת בוגרי 8200 מתגייסת למאבק בהשלכות הקורונה על ידי מתן שירותים שונים לציבור

עמותת בוגרי 8200 מציעים סיוע לציבור הרחב במספר קטגוריות שונות כמו: סיוע בהכנה לבגרויות, סיוע טכנולוגי לשירותי רפואה, שיחות טלפוניות לקשישים בודדים, ועוד. אנשים או ארגונים המעוניינים בסיוע העמותה יכולים לפנות אליה בכתובת המייל הבאה: support@8200.org.il.[9]

הרשות לניירות ערך מפרסמת הקלות לארגונים מדווחים על רקע התפשטות נגיף הקורונה

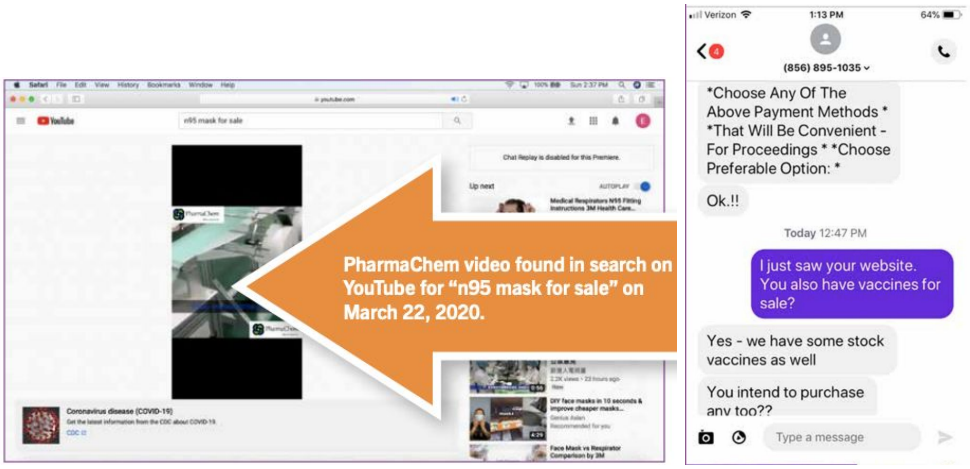
[6] https://onestore.nokia.com/asset/207324
[7] https://www.gov.il/he/departments/news/01042020_4
[8] https://www.nevo.co.il/law_word/law06/tak-8445.pdf
[9] https://www.8200.org.il/he/167

סגל רשות ניירות ערך פרסם היום מספר הקלות נוספות, בנוגע להתנהלות תאגידים שמחוייבים בדיווחים תקופתיים. הקלה אחת מתייחסת לארכה של 30 יום במועד פרסום הדוח הרבעוני לרבעון הראשון השנה, כך שמועד פרסומו יחול לא יאוחר מיום 30.6.2020, חלף 31.5.2020. חברות המיישמות את הארכה בפרסום הדוח, נדרשות לפרסם למשקיעים דוח מיידי במועד קבלת ההחלטה שלא להגיש את הדוח עד המועד הרגיל.[10] הקלה נוספת מאפשרת הארכת תקופת תשקיף המדף, כך שפקיעת תוקפו של אישור רגולטורי שהסתיים או צפוי להסתיים בין 10 למרץ עד ל-10 למאי, תידחה בחודשיים נוספים.[11]

סייבר וקורונה בעולם

גוגל סופגת ביקורת קשה על כך שמאפשרת מכירת מסכות וחיסונים מזוייפים כנגד נגיף הקורונה

חוקרים מ-Citizens Alliance ו-Coalition for a Safer Web תיעדו בחקירה ממושכת עשרות סרטונים ופרסומות בפלטפורמת הסרטונים 'Youtube' שהינה בבעלות גוגל, המציעים מסכות נשימה וחיסונים מזוייפים כנגד נגיף הקורונה. החוקרים קוראים לנקוט בצעדים משפטיים כנגד אלו שירוויחו ממשבר הקורונה.[12]



10 http://www.isa.gov.il/%D7%92%D7%95%D7%A4%D7%99%D7%9D%20%D7%9E%D7%A4%D7%95%D7%A7%D7%97%D7%99%D7%9D/Corporations/HodaotSegaL/General/Documents/2020_QuarterlyReportQ12020.pdf

11 http://www.isa.gov.il/%D7%92%D7%95%D7%A4%D7%99%D7%9D%20%D7%9E%D7%A4%D7%95%D7%A7%D7%97%D7%99%D7%9D/Corporations/Hodaot_segaL/Taskif_Azaot/Documents/application%20for%20extension%20of%20shelf%20prospectus.pdf

12 https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Corona_YouTube_Vaccines_3.30.20.pdf

מתיחות הקשורות בקורונה עלולות להוביל לעונשים ואף כלא

מדינות וארגונים רבים מזהירים מפני מתיחות הקשורות לקורונה באווירת ה-1 באפריל. גוגל, אשר ידועה במתיחות אשר מקיימת כל שנה בתאריך זה, ביטלה את המסורת עקב מגפת הקורונה אשר גבתה 40,000 קורבנות עד כה ברחבי העולם. מבין המדינות אשר מזהירות מפני הפצת פייק ניוז ומתיחות בנושאי הקורונה, תאילנד מאיימת להעמיד את העוברים על אזהרות אלו לדין שעונשו עד חמש שנות מאסר.[13]

בעלי אפליקציית Houseparty מציעים מיליון דולר לאדם שיוכיח כי פרצו את האפליקציה

בימים האחרונים ישנם שמועות רבות ברחבי המדיה החברתית על כך שאפליקציית Houseparty נפרצה. התומכים בדעה טוענים שבעקבות אותה פריצה, התוקפים הצליחו לחדור למשתמשי ה-Snapchat-וNetflix, Paypal, Spotify של הקורבנות, כמו גם לחשבונות בנק של משתמשים. EpicGames, החברה שיצרה את האפליקציה, מכחישה את השמועות בכל תוקף ואף פירסמה בטוויטר שלה Bounty של מיליון דולר לאדם אשר יצליח להוכיח כי האפליקציה אכן נפרצה.[14]

המועצה האוסטרלית לצרכנות מאגדת ענקיות תקשורת לצורך התמודדות עם עומס ברשת

המועצה האוסטרלית לצרכנות (ACCC) נתנה אישור לחמש חברות תקשורת לאגד משאבים פיננסיים עם הרשת האוסטרלית לצורך שיפור איכות הגלישה ברשת המדינית, עקב עלייה גדולה בשימוש בפלטפורמות אינטרנטיות.[15]

[13] https://www.reuters.com/article/us-health-coronavirus-april-fools/countries-threaten-jail-for-april-fools-day-jokes-about-coronavirus-idUSKBN21I2QH

[14] https://www.techradar.com/news/houseparty-offers-million-dollar-reward-to-prove-hacking-rumours-were-smear-campaign; https://www.thesun.co.uk/tech/11288862/houseparty-app-hacked-stealing-money-breach/

[15] https://www.zdnet.com/article/aussie-telco-heavyweights-create-group-to-handle-covid-19-network-surge/

פתרונות

מערך הסייבר הלאומי מפרסם תבנית לסקר סיכונים למגזר הקמעונאי

כחלק מהפעולות שביצע מערך הסייבר הלאומי לצורך תמיכה במשק הישראלי בעת משבר הקורונה, יצר המערך כלי עבודה שיהווה בסיס לביצוע סקר סיכוני סייבר עבור המגזר הקמעונאי. מטרת הסקר היא זיהוי סיכוני סייבר העלולים לפגוע בעסק, הערכת רמת הסיכון, הערכת סביבת הבקרה של מערכות מידע מהותיות ויצירת תמונת מצב עדכנית לצורך קבלת החלטות.[16]

ארגון MITRE פרסם מודל חדש בבסיס הידע שלו, ATT&CK, בנושא עבודה מקוונת

ארגון MITRE הינו ארגון ללא מטרות רווח המתמחה בהגנת סייבר. הארגון פרסם בעמוד הטוויטר של בסיס הידע שלו, ATT&CK, כי הקים מודל חדש בבסיס הידע בנושא עבודה מקוונת. כמו כן, קורא הארגון לקהילת אבטחת המידע ולעוקביו לאחד כוחות בתקופה זו, ולשתף מידע בפלטפורמת Twitter.[17]

העשרה

ארגון ללא מטרות רווח מדרג את עשרת המדינות אשר מטפלות בחולי קורונה הכי ביעילות, את המדינות הכי מסוכנות והכי בטוחות בתקופה זו

ארגון ללא מטרות רווח בשם Deep Knowledge Group, מספק לקהל הרחב ניתוח אנליטי שמדרג את המדינות ברחבי העולם לפי שלוש קטגוריות: עד כמה המדינות מטפלת ביעילות בחולי הקורונה, עד כמה המדינות מסוכנות לשהייה במהלך תקופת התפשטות מגפת הקורונה, ועד כמה המדינות בטוחות מבחינה רפואית. ניתוח המידע נאסף בצורה ידנית מאתרים המספקים נתונים סטטיסטיים כגון ארגון הבריאות העולמי, אוניברסיטת ג'ון הופקינס, ועוד.[18]

[16] https://www.gov.il/he/departments/policies/retailrisk

[17] https://twitter.com/MITREattack/status/1245350986081873920?ref_src=twsrc%5Etfw%7Ctwcamp%5Eembeddedtimeline%7Ctwterm%5Eprofile%3AMITREattack%7Ctwcon%5Etimelinechrome&ref_url=https%3A%2F%2Fattack.mitre.org%2F

[18] https://www.dkv.global/covid

שירותי סייבר בחינם לתקופת הקורונה

ריכזנו לנוחיותכם את המוצרים והשירותים בתחום הסייבר הניתנים בחינם במהלך תקופת הקורונה[19].
הטבלה מתעדכנת על בסיס יומי.

מספר	שם חברה	השירות המוצע
.1	Konfidas	חברת הייעוץ קונפידס מציעה הערכת סיכוני סייבר בחינם. ההערכה כוללת סקירה של אתר החברה והנכסים הדיגיטליים שלה, חשבונות מדיה חברתית המקושרים לעובדים בכירים והיבטי הרשת וטכנולוגיות המידע של החברה.
.2	Cygov	חברת CyGov מציעה שירות חינמי של תשתית בניית חוסן אבטחתי לחברות אשר עובדות מרחוק. במסגרת השירות מציעה החברה תוכנית לניהול סיכונים, הכוללת סט של חוקים אשר מטרתם לצפות ולנהל איומים במיוחד עקב משבר הקורונה.
.3	Domaintools	חברת Domaintools פרסמה דוח של כלל הדומיינים המזוייפים שנוצרים, אשר קשורים לנגיף הקורונה. על מנת להשאיר את מערכות ההגנה מעודכנות ככל הניתן, יש להזין דומיינים חשודים כדי לחסום גישה אליהם ולצמצם משמעותית את הסיכוי להיחשף להונאת הסייבר הבאה.
.4	Indusface	חברת Indusface הודיעה על מתן שירותי אבטחת מידע שונים לחברות שספגו פגיעה כתוצאה מווירוס הקורונה למשך חודש ללא עלות.
.5	coronavirusphishing	באתר החברה ניתן למצוא מידע אודות מרבית מתקפות הפישינג אשר פוקדות את העולם כתוצאה מהתפרצות נגיף הקורונה. המידע מחולק לפי נושאים: נשלח מטעם ארגון הבריאות העולמי, פייק ניוז, מכירת מוצרים מזויפים ועוד. ניתן לערוך בו חיפוש על פי מילות מפתח ולזהות אם נפלתם קורבן למתקפת פישינג.
.6	ITU	ה-ITU משיק פלטפורמה חדשה כדי לספק תמיכה למדינות בהתמודדותן עם היבטי סייבר של משבר הקורונה. הפלטפורמה מאפשרת שיתוף פעולה בין עשרות גורמים בכל העולם.

[19] המוצרים והשירותים המפורטים מטה מוצעים מטעם החברות עצמן ואין לראות בפרסום שלהם המלצה מטעם קונפידס לשימוש בהם.

.7	Global Cyber Alliance	החברה פרסמה "חבילות הגנה" חינמיות לצמצום נזקי סייבר. החבילה כוללת סדרת סרטונים המסכמים פעולות עיקריות שיש לבצע על מנת לצמצם את רמת החשיפה של ארגונים קטנים לאיומי סייבר.
.8	See Security	מכללת See Security מציעה לציבור הישראלי הזדמנות ללמוד קורס מקוון, "Introduction to Cybersecurity", ללא תשלום. הקורס מוצע בשיתוף עם חב' Cisco העולמית, ומעניק תעודת Cisco למסיימים בהצלחה.
.9	Proofpoint	חברת Proofpoint מציעה סט חינמי של חוקי IDS לזיהוי תקיפות הקשורות בנגיף הקורונה. יחידת המחקר של החברה זיהתה 42 חתימות של איומי סייבר הקשורים בנגיף הקורונה. חתימות המכילות מיילים, קבצי Word, דפי אינטרנט, חשבונות משתמשים ועוד.
.10	sndbox	חברת Sandbox מציעה מערכת חינמית אשר מיועדת לניתוח קבצים חשודים ושיתוף מידע בין חוקרים.
.11	Cyber Risk Aware	לאור עליה במתקפות הסייבר לצד התפשטות הקורונה, חברת Cyber Risk Aware מציעה לחברות לבצע תרגילי פישינג בחינם לעד כ-100 מעובדיהן.
.12	Minerva Labs	החברה מספקת פתרון הגנה ייחודי להגנה על המחשבים הביתיים המתחברים לארגון. הפתרון אינו מצריך התקנה, הרשאות או הפעלה מחדש של המחשב, ומגן על המחשב אך ורק לאורך החיבור לרשת הארגונית. בגמר ההתחברות, מירנווה נעלמת כלא הייתה, ובכך שומרת על הארגון מצד אחד ועל תקנות הפרטיות מצד שני. מינרווה נרתמת לעזור לעסקים בתקופה זו ומציעה את הפתרון ל-30 יום ללא עלות.
.13	מערך הסייבר הלאומי	מערך הסייבר הלאומי וקמפוס IL השיקו קורס חינמי, "מקדם הגנה בסייבר", לציבור הרחב. הקורס מקנה עקרונות בסיסיים כמו היכרות עם עולם הסייבר והסכנות המרכזיות שבו, כלים פשוטים לצמצום הסכנה, שיטות לזיהוי הנדסה חברתית ועוד.
.14	Odix	חברת Odix המפתחת ומספקת פתרונות ניטרול נוזקות (malware) המסתתרים בקבצים, תעניק לחברות רישיון לשימוש במוצר הלבנת קבצים לתקופה של 60 ימים חינם. פתרון Odix NetFolder מאפשר את הלבנת כל הקבצים המגיעים מפורטלים לרשת הארגונית. המערכת ניתנת להטמעה מהירה.
.15	Intezer	אינטזר פיתחה טכנולוגיה הנקראת Genetic Malware Analysis שמביאה בשורה מהפכנית לגילוי איומי סייבר על ידי מציאת המקורות הגנטיים של כל קוד תוכנה. אינטזר מאפשרת לארגונים לגלות איומי סייבר מודרניים, ומציעה פתרונות בתחומי אבטחת ענן

		ותגובה לאירועי סייבר.
.16	Orca Security	החברה מאפשרת לחברות בסקטורים שנפגעו (תיירות, מלונאות, אירועים ועוד) חצי שנה גישה חינם לפלטפורמת אבטחת הענן שלה.
.17	Cyber 2.0	החברה מספקת הגנה מהתפשטות התקפות סייבר בתוך הארגון ומחוצה לו, והיא תספק את המערכת שלה בענן או בהתקנה מקומית ללא עלות במהלך תקופת הקורונה.
.18	Rookout	חברת Rookout המפתחת מוצר ל-production debugging, מחלקת רשיונות חינם עד סוף 2020 לארגוני בריאות ורפואה הנלחמים בנגיף הקורונה

*** סוף המסמך ***

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