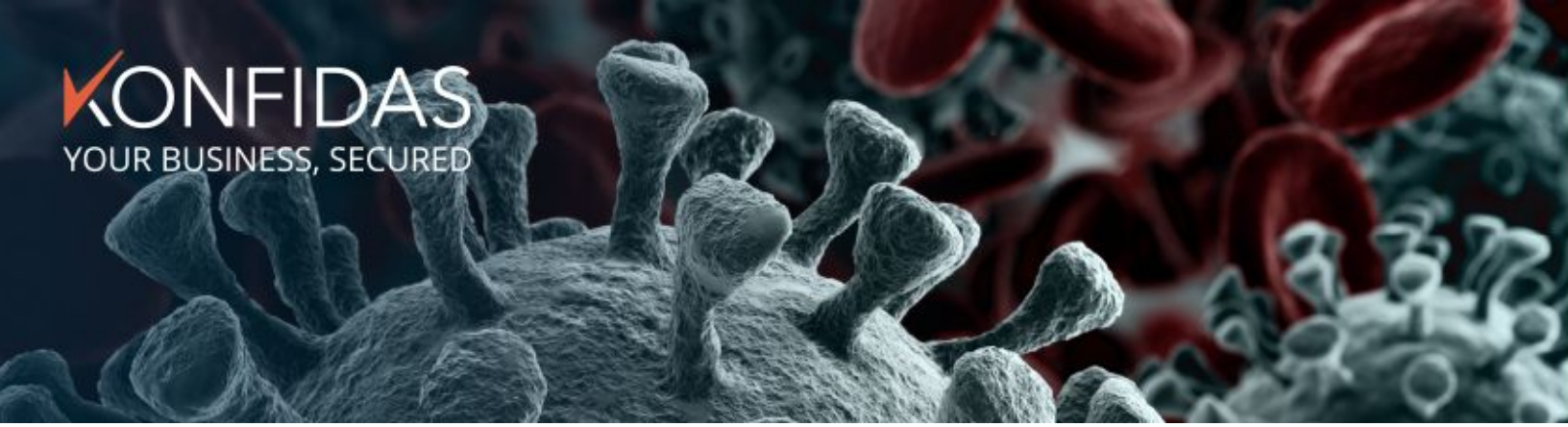

חדשות סייבר ונגיף הקורונה (COVID-19)

עדכון יומי ליום ב', 06.04.2020

הדוח מתפרסם גם במדור
"קפטן אינטרנט" של עיתון הארץ

הדוח מתפרסם גם בסייברנט

עיקרי הדברים

1. עליה של 50% בפניות למוקד המטה הלאומי להגנה על ילדים ברשת (105)
2. פערי אבטחה נוספים הנוגעים להצפנת שיחות Zoom
3. המלצות של מערך הסייבר הלאומי להגנה על הנתב הביתי
4. בשל נגיף הקורונה דחייה בקנסות GDPR ל-British Airways ו Marriott
5. נקודות מתוך ה- Webinar בנושא אתגרי הסייבר והפרטיות בצל נגיף הקורונה שהתקיים היום

31 Rothschild Blvd.Tel Aviv, 6578414
Office: +972-3-6444417 | info@konfidas.com | www.konfidas.com
© All Rights Reserved. Konfidas Digital Ltd.

תוכן עניינים

הציטוט היומי

איפה אפשר לקרוא את הדוחות?

איומים, התקפות והתראות

שני קמפייני פישינג חדשים מפיצים את הפוגענים LokiBot ו-AgentTesla

עליה של 50% בפניות למוקד המטה הלאומי להגנה על ילדים ברשת (105)

פערי אבטחה נוספים הנוגעים להצפנת שיחות Zoom

סייבר וקורונה בישראל

משטרת ישראל מתכננת להשתמש בתוכנה לאיתור התקהלויות

מערך הסייבר הלאומי העלה לאוויר את ה-Marketplace לחברות סייבר

סייבר וקורונה בעולם

הפסדים של £1.6M בעקבות הונאות הקשורות לנגיף הקורונה באנגליה

בשל התפשטות נגיף הקורונה, דחייה בהטלת קנסות ה-GDPR על British Airways ו-Marriott

מיקרוסופט פועלת בשיתוף פעולה עם ארגוני בריאות לצורך התמודדות עם מתקפות כופרה

בזכות התערבות של היורופול נעצר בסינגפור חשוד בגין הונאה בסך 6$ מיליון

פתרונות

חברת NordVPN מגרילה חודש או שנה חינם וזאת ברכישת רישיון למשך 3 שנים

חברת Palo Alto מפרסמת טיפים לקיום שיחת וידאו מאובטחת

העשרה

נקודות מתוך ה- Webinar בנושא אתגרי הסייבר והפרטיות בצל נגיף הקורונה

שירותי סייבר בחינם לתקופת הקורונה

© All Rights Reserved. Konfidas Digital Ltd.

הציטוט היומי

"לחסום בתי חולים ממערכות המחשוב הקריטיות שלהם, לא רק תעכב את הטיפול הרפואי המהיר הדרוש בזמנים חסרי תקדים אלה, אלא עלול עלולה להוביל ישירות למקרי מוות."[1]

(קים ג'ונג יאנג, נשיא האינרטפול,

בהתייחסות היום למתקפות כופרה על בתי חולים ברחבי העולם)

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://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

© All Rights Reserved. Konfidas Digital Ltd.

איומים, התקפות והתראות

שני קמפייני פישינג חדשים מפיצים את הפוגענים LokiBot ו-AgentTesla

חברת F-Secure מזהה מגמה של מיקוד התחבולות של גורמים זדוניים בנושא העבודה מרחוק. החברה זיהתה שני קמפייני פישינג חדשים, הראשון שבהם מתחזה למייל המכיל בתוכו מידע חשוב על תוכנית המשכיות עסקית, ומצורף אליו קובץ שבעת הורדתו מופעל פוגען LokiBot. הקמפיין השני מתחזה למייל המציג מידע בנוגע להסגר ודורש מהנמען לשלם סכום כסף לטובת חיטוי כלל המכולות שנכנסות ויוצאות מהנמל. למייל מצורף קובץ עם פוגען בשם AgentTesla.[2]

עליה של 50% בפניות למוקד המטה הלאומי להגנה על ילדים ברשת (105)

ביחידה המשטרתית 105 של להב 433, המהווה את המטה הלאומי להגנה על ילדים ברשת, נרשמה עליה של כ-50% בכמות השיחות שהתקבלו במוקד 105. המידע שנמסר על ידי המטלפנים כולל דיווחים על מעשים פליליים כמו הפצת סרטונים ותמונות אינטימיות וביצוע עבירות מין, לצד דיווחים על פגיעות שאינן פליליות, כגון ביוש (שיימינג). המשטרה קוראת לציבור לגלות מעורבות ואחריות למעשיהם, וממליצה להורים לשוחח עם ילדיהם ולוודא כי הם מבינים את הסכנות הקיימות ברשת.

פערי אבטחה נוספים הנוגעים להצפנת שיחות Zoom

בהמשך לדיווחים הרבים הנוגעים לפגיעויות ופערי אבטחה בפלטפורמת הפגישות המקוונות Zoom, בדוח של חברת Citizen Lab מתפרסמת חקירה החושפת שני פערי אבטחה נוספים, הפעם בהצפנה בה משתמשת הפלטפורמה. ראשית, נעשה שימוש בסוג הצפנה שאינו מומלץ, זאת בניגוד לתיעוד הרשמי של האפליקציה, בו מצוין כי נעשה שימוש בסוג הצפנה מתקדם יותר. עוד התגלה שימוש מטעה במונחי הצפנה ואבטחה שאינו תואם את משמעויותיהם, לדוגמה "הצפנת קצה לקצה".

שנית, מפתחות הפענוח של ההצפנה, אשר מיוצרים על ידי שרתים של חברת Zoom, עוברים בחלק מהמקרים דרך שרתים בסין, זאת על אף שאיש ממשתתפי השיחה אינו נמצא בסין. בבעלותה של חברת Zoom, הממוקמת בעמק הסיליקון, שלוש חברות הממוקמות בסין, אשר אחראיות על פיתוח התוכנה של הפלטפורמה. לכן, בממצאי החקירה שפורסמו מציינת חברת Citizen Lab שהעברת המפתחות דרך סין מדאיגה, זאת משום שהחברה עצמה עלולה להיות נתונה ללחץ ודרישות מצד ממשלת סין.[3]

[2] https://blog.f-secure.com/coronavirus-spam-update-watch-out-for-these-emails/

[3] https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/ ; https://twitter.com/RonDeibert/status/1246038249832931328

© All Rights Reserved. Konfidas Digital Ltd.

סייבר וקורונה בישראל

המלצות של מערך הסייבר הלאומי להגנה על הנתב הביתי

מערך הסייבר הלאומי פרסם היום, המלצות לאזרח להגנה על נתב האינטרנט הביתי. בין ההמלצות מפורטים צעדים להקשחת הגדרות הנתב, ביצוע עדכונים עיתיים לנתב, הפעלת חומת אש (Firewall), הגדרת רשת נפרדת לאורחים, הגדרת רמת הצפנה גבוהה למידע העובר על גבי הרשת ועוד.

משטרת ישראל מתכננת להשתמש בתוכנה לאיתור התקהלויות

המשטרה פנתה לחברות אזרחיות בבקשה שיציעו לה תוכנות לאיתור התקהלויות של יותר מ-50 איש, כדי שיתריעו בפניה על התרחשותן "בזמן קרוב לאמת", לצורך אכיפת הנחיות משרד הבריאות בצורה יעילה. גורמים הבקיאים בנושא אמרו כי מדובר במערכות שמבצעות איכון לטלפונים ניידים, אולם לפי הודעת המשטרה - המערכות לא יאספו פרטים אישיים על בעלי המכשירים.[4]

מערך הסייבר הלאומי העלה לאוויר את ה-Marketplace לחברות סייבר

בעקבות משבר הקורונה הקים מערך הסייבר הלאומי marketplace, בו ניתן למצוא חברות המציעות שירותים ומוצרים להגנת סייבר בהטבות משמעותיות, בחלוקה לקטיגוריות: https://go.gov.il/marketplace

סייבר וקורונה בעולם

הפסדים של £1.6M בעקבות הונאות הקשורות לנגיף הקורונה באנגליה

המרכז הלאומי לדיווח על הונאות ופשעי סייבר בבריטניה, Action Fraud, קיבל עד כה 509 דיווחים על קמפיינים מזויפים הקשורים לנגיף הקורונה. עד כה, שולמו בסך הכל £1.6M בעקבות מספר קמפיינים מזוייפים, המבקשים תרומה להתמודדות עם המגפה, או דורשים תשלום קנס בעקבות התנהגות המפרה תקנות שנקבעו להתמודדות עם נגיף הקורונה. בין הקמפיינים הבולטים מצוי דואר אלקטרוני מזויף אשר מגייס, כביכול, תרומות לארגון שירות הבריאות הלאומי בבריטניה (NHS) לצורך רכישת ציוד אספקה רפואי והכנות רפואיות להתמודדות עם מגפת הקורונה.[5]

[4] https://www.haaretz.co.il/health/corona/.premium-1.8742315
[5] https://www.theguardian.com/world/2020/apr/04/fraudsters-exploiting-covid-19-fears-have-scammed-16m

© All Rights Reserved. Konfidas Digital Ltd.

בשל התפשטות נגיף הקורונה, דחייה בהטלת קנסות ה-GDPR על British Airways ו-Marriott

נציבות הגנת המידע הבריטית דוחה שוב את הטלת הקנסות בגובה 280 מיליון פאונד על בריטיש איירווייס ורשת מלונות מריוט בגין דליפות נתונים. הקנסות הוטלו על שתי החברות בעקבות פריצות למערכות המחשוב שלהן, שפגעו במיליוני אנשים ברחבי העולם. הקנסות של מריוט עוכבו עד ה-1.6.2020, ותאגיד International Airlines Group: IAG (המחזיק ב British Airways) חשף בדו"ח הכספי שלו כי הקנס שלהם ידחה עד ל-18.5.2020.

מיקרוסופט פועלת בשיתוף פעולה עם ארגוני בריאות לצורך התמודדות עם מתקפות כופרה

עקב המעבר לעבודה מהבית, מתקפות כופרה שמות דגש על מטרה ממוקדת: רכיבי תקשורת המהווים שער כניסה לרשת, כמו VPN או נתבים. בעיקר מתמקדות תקיפות הכופרה בעובדי הסקטור הרפואי. כתוצאה מכך, מיקרוסופט משקיעה את מאמציה בזיהוי תקיפות כופרה המכוונות לרכיבי VPN, ובאופן ספציפי מתמקדת במתקפת כופרה בשם REvil. זאת ועוד, מיקרוסופט שלחה בצורה אקטיבית הודעות ייעודיות לבתי חולים עם מידע אודות חולשות ב-VPN ורכיבי תקשורת אחרים לצורך מניעת המתקפות.[6]

בזכות התערבות היורופול נעצר בסינגפור חשוד בגין הונאה בסך 6$ מיליון

החשוד, בן 39, נעצר בסינגפור בחשד למעורבות בהונאת מייל, אשר הובילה משתמשים לאתר זדוני בו נמכרו, כביכול, מסכות ומוצרי חיטוי. המעצר הגיע בתגובה לדיווח על הונאה של חברת תרופות אירופאית בסכום כולל של 6.64 מיליון דולר.[7]

חברת ProPublica זיהתה פרופילי טוויטר מזויפים המקושרים לממשלת סין ומפיצים מידע כוזב על נגיף הקורונה

חברת ProPublica זיהתה מאז אוגוסט 2019 יותר מ-10,000 חשבונות טוויטר החשודים כמזויפים. החשבונות הפיצו בעבר מסרים התואמים את העמדות של ממשלת סין, ואילו כיום זוהו כמפיצים מידע תעמולתי אודות המשטר הסיני ו/או הקורונה, וחלקם אף מידע שקרי בנוגע להתפרצות הנגיף.[8]

פתרונות

חברת NordVPN מגרילה חודש/שנה חינם ברכישת רישיון למשך 3 שנים

החברה, המספקת שירותי VPN, פתחה במבצע אשר במסגרתו כל מי שירכוש רישיון לתוכנת ה-VPN שלה למשך שלוש שנים יוכל להשתתף בהגרלה בה יוענקו לזוכים חודש או שנה שלמה של שימוש בתוכנה בחינם.[9]

[6] https://www.microsoft.com/security/blog/2020/04/01/microsoft-works-with-healthcare-organizations-to-protect-from-popular-ransomware-during-covid-19-crisis-heres-what-to-do/
[7] https://www.europol.europa.eu/newsroom/news/corona-crimes-suspect-behind-%E2%82%AC6-million-face-masks-and-hand-sanitisers-scam-arrested-thanks-to-europol-intervention
[8] https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus
[9] https://nordvpn.com/easter/?utm_medium=affiliate&utm_term&utm_content&utm_campaign=off24&utm_source=aff8376&utm_expid=.4kmAXWQmQ1qQJoQBsCNXzQ.1&utm_referrer=

© All Rights Reserved. Konfidas Digital Ltd.

חברת Palo Alto מפרסמת טיפים לקיום שיחת וידאו מאובטחת

לאור העלייה החדה בשימוש בפלטפורמות שונות לביצוע שיחות וידאו, פרסמה חברת פאלו אלטו מספר טיפים לצורך ביצוע שיחות וידאו בצורה מאובטחת. בין הטיפים: יישום אופציה של סיסמת גישה לשיחה בכל שימוש בפלטפורמה, אימות של כלל המשתתפים בשיחה, וידוא כי הפלטפורמה מתעדכנת על בסיס יומי ועוד.[10]

העשרה

נקודות מתוך ה- Webinar בנושא אתגרי הסייבר והפרטיות בצל נגיף הקורונה

היום התקיים webinar משותף של החברות Konfidas ו-ISACA ישראל בנושא אתגרי הסייבר והפרטיות בצל משבר הקורונה. 120 אנשים הצטרפו לשמוע את המומחים מדברים על האתגרים והתובנות מהמשבר. התובנות העיקריות שעלו מהווביונר:

לדברי איל בן עמרם, CIO ב"צים", סין חזרה לייצר בקצב שקדם להתפרצות הקורונה, אך רמת הביקוש בארצות הברית לא ברורה. אם ארצות הברית תכנס למשבר חריף בעקבות הקורונה, תהיה לכך השפעה מהותית על השוק העולמי.

לביא שטוקהמר, ראש ה-CERT הלאומי, ציין שקיימת עלייה של 300% בחיבורים מרחוק בישראל, מה שמייצר סביבת תקיפה נוחה לגורמים זדוניים. עם זאת, רמת ההגנה והמוכנות של ארגונים בישראל הינה ברף המתקדם ביותר וכוללת הבנה טובה יותר של הצד התוקף, ביחס למדינות אחרות. בנוסף, הראוטר הפך להיות נקודת גישה לתוך הרשת הארגונית ולכן יש להקשיח את הראוטרים ולהגן עליהם.

שוקי פלג, חבר מועצה ב-ISACA ישראל ו-CISO של קבוצת הבינלאומי, ציין כי פריסת העבודה מרחוק התבצעה תוך ימים בודדים, לעומת מצב שגרתי בו היה לוקח חודשים לפרוס תשתית דומה.

בנושא הגנת הפרטיות אמר עו"ד אסף הראל, שותף ב"גורניצקי ושות'", שארגונים אינם ערוכים די הצורך ברמה החוזית ואין בהם התייחסות לנושא "כוח עליון" אשר מתיר הפרת חוזה בסיטואציות קיצוניות, כמו זו של התפרצות נגיף הקורונה.

שי סימקין, ראש תחום סייבר של קבוצת "האודן" בעולם, ציין כי הוא מקבל הרבה פניות בנוגע לשאלה האם ביטוחי הסייבר מכסים עבודה מרחוק. סימקין מאשר כי ביטוח סייבר מכסה עבודה מרחוק, גם אם המצב הנוכחי שונה מאד ממצב התשתיות והפעילות שהיו כאשר הביטוח נרכש.

[10] https://blog.paloaltonetworks.com/2020/04/network-video-conferencing-security/

© All Rights Reserved. Konfidas Digital Ltd.

שירותי סייבר בחינם לתקופת הקורונה

ריכזנו לנוחיותכם את המוצרים והשירותים בתחום הסייבר הניתנים בחינם במהלך תקופת הקורונה.[11]
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. החברה מפעילה מוקד חירום לאירועי סייבר בטלפון 03-6444414 או במייל Attackhelp@konfidas.com . בנוסף, החברה מעניקה בחינם הרצאות מרחוק בנושא המודעות לסיכוני הסייבר בצל הקורונה.
.2	Cygov	חברת CyGov מציעה שירות חינמי של תשתית בניית חוסן אבטחתי לחברות שעובדות מרחוק. במסגרת השירות מציעה החברה תוכנית לניהול סיכונים, הכוללת סט של חוקים שמטרתם לצפות ולנהל איומים במיוחד עקב משבר הקורונה.
.3	Domaintools	חברת Domaintools פרסמה דוח של כלל הדומיינים המזוייפים שנוצרים בהקשר של נגיף 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 שפוקדות 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 המספקת תמיכה למדינות בהתמודדותן עם היבטי סייבר של משבר הקורונה. הפלטפורמה מאפשרת שיתוף פעולה בין עשרות גורמים בכל העולם.

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

© All Rights Reserved. Konfidas Digital Ltd.

.7	Global Cyber Alliance	החברה פרסמה "חבילות הגנה" חינמיות לצמצום נזקי סייבר, הכוללת 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 ללא תשלום בנושא "Introduction to Cybersecurity"., הקורס מוצע בשיתוף עם חברת Cisco העולמית, ומעניק תעודת Cisco למסיימים אותו 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 לנגיף, ביניהן חתימות המכילות מיילים, קבצי Word, דפי אינטרנט, חשבונות משתמשים ועוד.
.10	sndbox	חברת Sandbox מציעה מערכת חינמית שמיועדת 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 ייחודי להגנה על המחשבים הביתיים המתחברים לארגון. הפתרון אינו מצריך התקנה, הרשאות או הפעלה מחדש של המחשב, והוא מגן על המחשב אך ורק לאורך החיבור לרשת הארגונית. בגמר ההתחברות, החברה 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) המסתתרות 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 המכונה Genetic Malware Analysis, שמביאה בשורה מהפכנית של גילוי איומי סייבר על ידי מציאת המקורות הגנטיים של כל קוד תוכנה. אינטזר מאפשרת לארגונים לגלות איומי סייבר מודרניים, ומציעה פתרונות בתחומי

© All Rights Reserved. Konfidas Digital Ltd.

		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 מפני התפשטות 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.
.19	SafeHouse	אפליקציית ההגנה מבית SafeHouse, שמקנה הגנה ופרטיות ברשת, שומרת עליכם בכל זמן ובכל מקום, במיוחד עכשיו. לנוכח המצב והשימוש המוגבר בטלפונים ניידים ועבודה מהבית, החברה מעניקה למשתמשים בישראל חודש שימוש בחינם.
.20	CyberArk	חברת סייברארק מציעה את CyberArk Alero, פתרון שנועד לספק גישה פריבילגית קלה ומאובטחת למשתמשים מרוחקים, לרבות עובדים וספקי צד שלישי. CyberArk Alero משלב בפתרון אחד גישת אפס אמון, אימות זהות ביומטרי והקצאת גישה just-in-time, ללא צורך ב-VPN, התקנת תוכנה (agents) או סיסמאות. כך מתאפשרת גישה מאובטחת לעובדים מרוחקים למערכות קריטיות המנוהלות על ידי סייברארק. הפיתרון מוצע בחינם עד סוף חודש מאי ללקוחות סייברארק.
.21	KAPE	החברה, המתמחה בהצפנה של מידע דיגיטלי ופתרונות גלישה אנונימית, מציעה שימוש חינמי עד סוף תקופת ההסגר ברשת וירטואלית פרטית (VPN), המאפשרת גלישה אנונימית מאובטחת המגינה על פרטיות המשתמש.

*** סוף המסמך ***

31 Rothschild Blvd.Tel Aviv, 6578414
Office: +972-3-6444417 | info@konfidas.com | www.konfidas.com
© All Rights Reserved. Konfidas Digital Ltd.