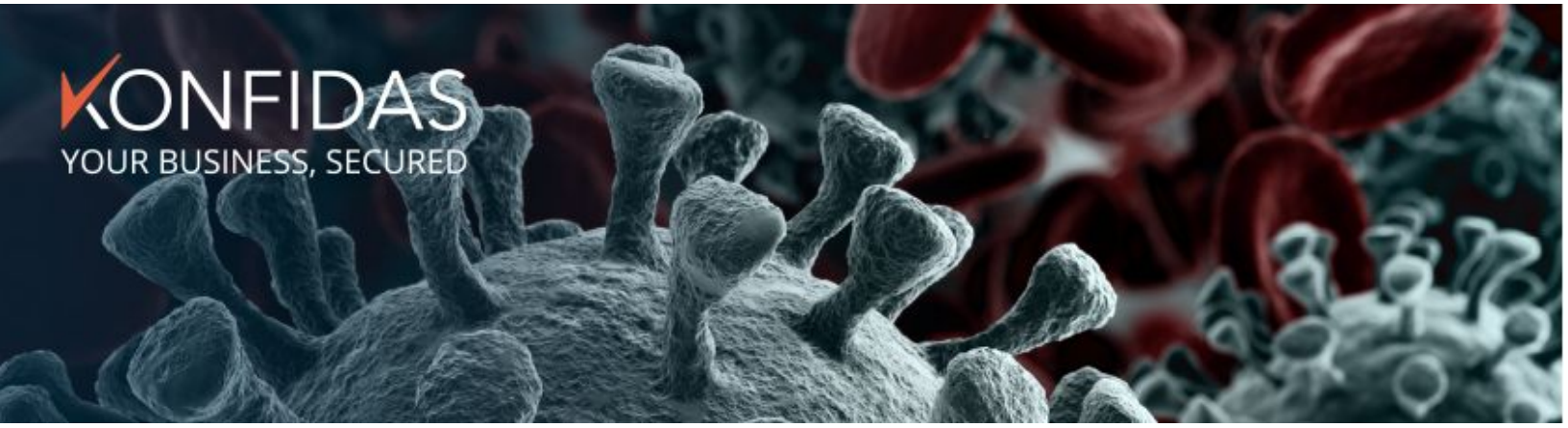


חדשות סייבר ונגיף הקורונה (COVID-19)

עדכון יומי ליום א׳, 5.04.2020

הדוח מתפרסם גם במדור "קפטן אינטרנט" של עיתון הארץ

הדוח מתפרסם גם בסייברנט

עיקרי הדברים

1. האינטרפול פרסם אזהרה מפני מתקפות סייבר על מוסדות בריאות ומסייע בהתמודדות עמן.
2. משטרת ישראל מדווחת על פעילות פישינג המתחזה לשירותי Netflix ו-Paypal.
3. מאמצים למניעת מכירת חיסונים מזויפים כנגד הקורונה גם בדארקנט.
4. ביום שני יתקיים Webinar משותף ל-ISACA ו-Konfidas בנושא אתגרי הסייבר והפרטיות בצל נגיף הקורונה.

31 Rothschild Blvd.Tel Aviv, 6578414

Office: +972-3-6444417 | info@konfidas.com | www.konfidas.com

תוכן עניינים

הציטוט היומי

" פישלנו בגדול בעניין האבטחה. אוי לנו אם נפשל שוב."

אריק יואן, מנכ"ל Zoom

איפה אפשר לקרוא את הדוחות?

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

טוויטר:
https://twitter.com/konfidas

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

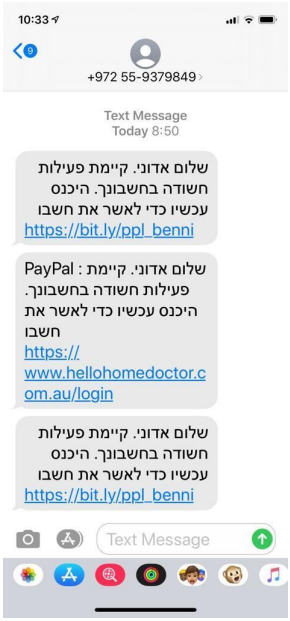
אתר האינטרנט של קונפידס:
https://www.konfidas.com

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

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

איומים, התקפות והתראות

משטרת ישראל מדווחת על פעילות פישינג המתחזה לשירותי Netflix ו-Paypal



יחידת הסייבר במשטרת ישראל, להב 433, דיווחה על פעילות של תשתית פישינג שמטרתה לאסוף פרטי מידע וחשבונות מאזרחים ישראליים. התקיפה התבצעה באמצעות שליחת מסרוני SMS המבקשים לעדכן את פרטי התשלום לתוכנת Netflix ומכילים קישורים מזויפים ל-Netflix ול-PayPal.

נוסח ההודעות המתחזות לחברת Netflix:

- לא הצלחנו לעבד את התשלום האחרון שלך. כדי להמשיך ולהנות מ-Netflix, יש לעדכן את פרטי התשלום opu57.com?Netflix.com

נוסח ההודעות המתחזות לחברת Paypal:

- שלום אדוני. קיימת פעילות חשודה בחשבונך, היכנס עכשיו כדי לאשר את החשבון https://bit.lyy/ppl_benni
- PayPal שלום אדוני. קיימת פעילות חשודה בחשבונך, היכנס עכשיו כדי לאשר את החשבון https://www.hellohomedoctor.com.aus/login
- שלום אדוני. קיימת פעילות חשודה בחשבונך, היכנס עכשיו כדי לאשר את החשבון https://bit.lyy/ppl_securt

אנו חוזרים וממליצים להיכנס לחשבונות ואתרים רק באמצעות קישורים רישמיים.

11 אפליקציות זדוניות שלכאורה מאפשרות מעקב אחר התפשטות נגיף הקורונה

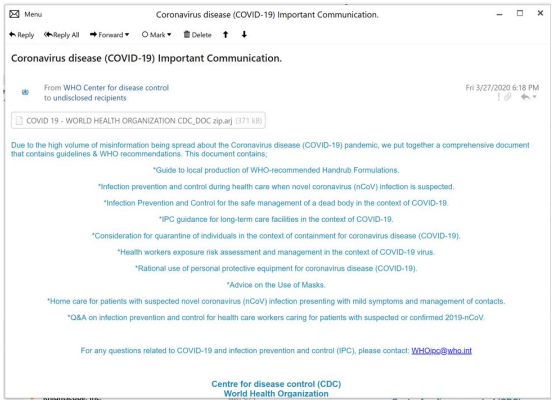
צוות המחקר של חברת Symantec זיהה 11 אפליקציות אשר מתחזות לאפליקציה אחת, שמטרתה להעריך את הסיכון להתפשטות הנגיף על פי מספר המודבקים. האפליקציות המתחזות שמרו על מאפייני האפליקציה המקורית ודורשות מידע על מיקום המשתמש לצורך ניטור התפשטות הנגיף. אלא שאותן אפליקציות מזויפות מכילות קטעי קוד זדוניים, המאפשרים גניבה של מידע, כדוגמת הודעות SMS ואנשי קשר, ואפילו לקיחת צילומי מסך (screenshot) מהמכשיר הסלולרי. ניתן למצוא מזהים (IOCs) בסימוכין.[1]

מתקפת פישינג חדשה מצליחה לעבור את הבקרות של Proofpoint ו-Microsoft 365

חברת Cofense זיהתה מתקפת פישינג אשר חדרה לדומייני המייל המאובטחים של Microsoft 365 ו-Proofpoint. קמפיין הפישינג החדש הצליח לחדור למייל דרך אמצעי הגנה בסיסיים באמצעות זיוף (spoofing) דומיין שולח המייל לזה של ארגון הבריאות העולמי (WHO). המייל, אשר קרא למשתמשים להתעדכן במיקומי חולי קורונה בעיר מגוריהם, הכיל לינק לאתר המתחזה לאתר Microsoft, בכדי לגנוב את פרטי משתמש ה-Windows שלהם.[2]

[1] https://symantec-blogs.broadcom.com/blogs/threat-intelligence/android-apps-coronavirus-covid19-malicious
[2] https://cofense.com/threat-actors-evade-proofpoint-office-365-atp-protection-capitalize-covid-19-fears/

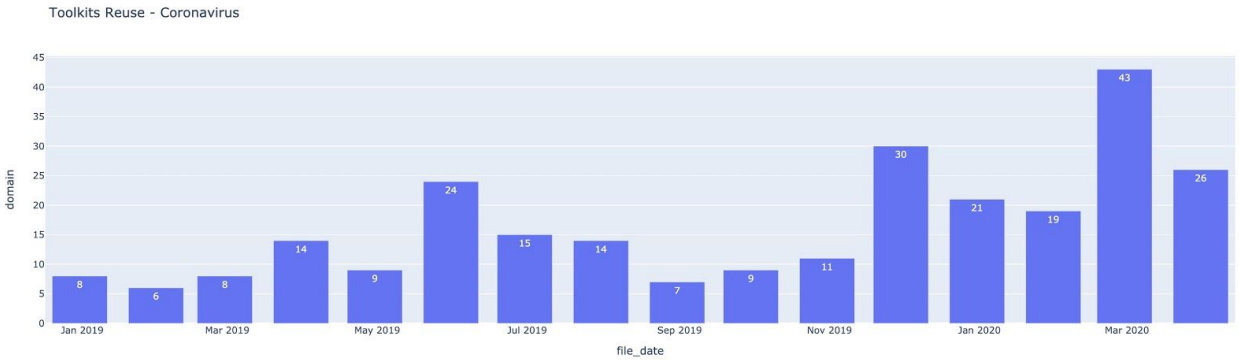
קמפיין פישינג ממוקד מנצל את נגיף הקורונה להפצת פוגען מסוג גניבת מידע



חברת Fortinet חשפה קמפיין פישינג ממוקד (spear phishing) שמתחזה לארגון הבריאות העולמי. המייל מכיל מסר מארגון הבריאות העולמי ופעולות שיש לבצע על מנת לצמצם את ההדבקה. זאת ועוד, למייל מצורף קובץ שבעת פתיחתו רץ על המחשב המותקף פוגען בשם "LokiBot", שנועד לגנוב מידע מהמחשב, כגון פרטי הזדהות, סיסמאות מייל, סיסמאות השמורות בדפדפן ועוד. ניתן למצוא מזהים בסימוכין.[3]

מִחזור מתקפות פישינג לצורך ניצול משבר הקורונה

חוקרים של חברת Akamai מדווחים כי למרות רישומי דומיינים רבים בהקשר לקורונה, הכלים שעומדים מאחורי מתקפות הפישינג הם כלים ישנים אשר כבר נראה בעבר שימוש בהם. לצד העלייה במתקפות הפישינג, ניתן לראות במִחזור כלי התקיפה יתרון, כיוון שכלי ההגנה יודעים להתמודד איתם. בגרף הבא ניתן לראות עלייה חדה במִחזור כלי תקיפה לאחר התפרצות הקורונה.[4]



[3] https://www.fortinet.com/blog/threat-research/latest-global-covid-19-coronavirus-spearphishing-campaign-drops-infostealer.html
[4] https://blogs.akamai.com/sitr/2020/04/threat-actors-recycling-phishing-kits-in-new-coronavirus-covid-19-campaigns.html

סייבר וקורונה בישראל

משטרת ישראל תאפשר הגשת תלונה באופן אינטרנטי

החל ממחר בבוקר, יום שני ה-06.04.2020, תאפשר משטרת ישראל הגשת תלונה דרך אתר האינטרנט הרשמי שלה, מבלי להגיע פיזית לתחנת משטרה. השירות החדש מושק על מנת לצמצם את הסכנה הבריאותית הנשקפת לאזרחים ולשוטרים כאחד, כמו גם לצורך שיפור השירות הניתן לאזרחים.[5]

סייבר וקורונה בעולם

האינטרפול פרסם אזהרה מפני מתקפות סייבר על מוסדות בריאות ומסייע בהתמודדות עמן

האינטרפול מזהיר מפני מתקפות סייבר מכוונות על מוסדות וגופים רפואיים, בכללם בתי חולים. האזהרה מתמקדת במתקפות כופרה, בהן ימנעו התוקפים את שימוש הגופים במערכות קריטיות עד לקבלת תשלום. בהמשך לאזהרה, פרסם האינטרפול כי גוף התגובה שלו לאיומי סייבר (INTERPOL's Cybercrime Threat Response Team) עובד בשיתוף עם כוחות המשטרה ואף עם גופים פרטיים על מנת לאסוף מודיעין מקדים על המתקפות, לחקור אותן ולסייע לקורבנותיהן. נוסף על כך, האינטרפול פרסם מספר צעדים בהם יש לנקוט כדי להתגונן מפני התקיפות, כגון עדכון תוכנות אנטי-וירוס, שימוש בסיסמאות ייחודיות וחזקות, הימנעות מכניסה לקישורים/מיילים חשודים, ועוד.[6]

משטרת הולנד סגרה 10 אתרי שמכרו ציוד מזויף לטיפול בקורונה והוציאה אזהרה בנושא

האתרים, שהופעלו על ידי פושעי סייבר, הציעו מוצרים כגון כרטיסי בנק אנטי-בקטריאליים, אפליקציות איתור קורונה ומסכות פנים. כמה מהאתרים גנבו שמות של אתרים ידועים ואילו האחרים היו מזוייפים לחלוטין.[7]

מאמצים למניעת מכירת חיסונים מזויפים כנגד הקורונה גם בדארקנט

הפורום Monopoly Market, המהווה פלטפורמה למכירת סמים לא חוקיים בדארקנט, אוסר על מכירת חיסונים ותרופות מזויפות כנגד הקורונה. בהצהרה שפירסמו בעלי הפורום, הם מוסיפים כי כל משתמש אשר יציע למכירה מוצר שיש בו מחסור, כמו נייר טואלט ומסכות, יוסר לאלתר מהפורום. עוד הם מציינים שהפורום לא ייתן יד לשימוש בקורונה כאמצעי שיווקי.[8]

[5] https://www.gov.il/he/departments/news/police_5-4-20_online_complaint

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

[7] https://www.dutchnews.nl/news/2020/04/dutch-police-take-10-corona-fraud-webshops-off-line/

[8] https://www.independent.co.uk/life-style/gadgets-and-tech/news/coronavirus-vaccine-cure-dark-web-drugs-market-covid-19-a9442671.html

גוגל פרסמה מידע על מיקום המשתמשים שלה ב-131 מדינות לצורך בחינת הצלחת הבידוד

בדוח שפורסם מציגה גוגל מידע על מיקום משתמשיה מה-16 בפברואר ועד סוף מרץ במקומות כמו חנויות, תחבורה ציבורית, סופרים ועוד. מהדוח ניתן לראות כי באיטליה הייתה ירידה של 94% בהימצאות תושבים באזורי קמעונאות ובילוי, לעומת ירידה של פחות מ-50% בארצות הברית.[9]

פתרונות

מערך הסייבר הלאומי מפרסם המלצות לשימוש בתוכנת Zoom

עקב מגפת הקורונה והמעבר לעבודה מרוחקת של מרבית המשק בישראל ובעולם, נוספו לתוכנת Zoom מיליוני משתמשים חדשים. הפופולריות של התוכנה הופכת אותה למטרה נגישה להאקרים רבים ברחבי העולם. זאת ועוד, בשבוע האחרון דווח על חולשת Zero Day בפלטפורמה, שנסגרה בעדכון הגרסה האחרון של שלה. בעקבות כך פרסם מערך הסייבר המלצות לשימוש ב-Zoom, ביניהן: פרסום על קיום הפגישה באמצעים פנים ארגוניים, נעילת הפגישה לאחר הצטרפות כלל המשתתפים ועוד.[10]

ביום שני יתקיים Webinar משותף ל-ISACA ו-Konfidas בנושא אתגרי הסייבר והפרטיות בצל נגיף הקורונה

חברת Konfidas בשיתוף עם ISACA מזמינות אתכם להשתתף בסמינר מקוון (Webinar) בו ידונו באתגרים של ארגונים בתקופת הקורונה, בשימוש באמצעים טכנולוגיים, בשינוי תהליכי עבודה בארגון ובהתמודדות עם איומי הסייבר בצל המשבר. הסמינר יתקיים ביום שני ה-6.4.2020 בשעה 17:00. להרשמה לחצו על הלינק.

העשרה

מומחי פרטיות מודאגים מהאפליקציה החדשה של NSO

לפני כשבועיים הכריזה NSO על פיתוח אפליקציה אשר תעקוב אחר התפשטות נגיף הקורונה לצורך הפקת תחזיות התפרצות ותמיכה בהחלטות ממשלתיות בנושא. קבוצת NSO בנתה את האפליקציה באמצעות קטע קוד לריגול שאותו בנתה בעבר לצורך פוגען המכונה "פגסוס". חוקרים אינם רואים בעין יפה שימוש ממשלתי לצורך צמצום המגפה בכלי אשר שימש בעבר לריגול.[11]

[9] https://www.google.com/covid19/mobility/
[10] https://www.gov.il/BlobFolder/reports/zoom_recommendation/he/ZOOM-CERT-IL-W-1049.pdf
[11] https://www.vice.com/en_us/article/epg9jm/nso-covid-19-surveillance-tech-software-tracking-infected-privacy-experts-worried

שירותי סייבר בחינם לתקופת הקורונה

ריכזנו לנוחיותכם את המוצרים והשירותים בתחום הסייבר הניתנים בחינם במהלך תקופת הקורונה.[12]
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
.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.

[12] 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, 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

		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