חדשות סייבר ונגיף הקורונה (COVID-19)

עדכון יומי ליום ג', 31.03.2020

הדוח מתפרסם גם במדור
"קפטן אינטרנט" של עיתון הארץ

הדוח מתפרסם גם בסייברנט

עיקרי הדברים

1. FBI מפרסמת אזהרה מפני חדירה לשיחות ועידה בפלטפורמת ZOOM.
2. משטרת ישראל מזהירה מפני ניסיונות סחיטה וירטואליים.
3. פרקליטות המדינה שוקלת העמדה לדין בגין הפצת פייק ניוז.
4. המלצות IT וסייבר לשדות התעופה בעקבות השיבושים שנגרמו ממגפת הקורונה.
5. הרע לפנינו? שיח נרחב על הקורונה בדארקנט, כולל תכנונים למתקפות פישינג.
6. צילום מסך של ועידת ZOOM בה נכח ראש ממשלת אנגליה חשף את פרטי הפגישה

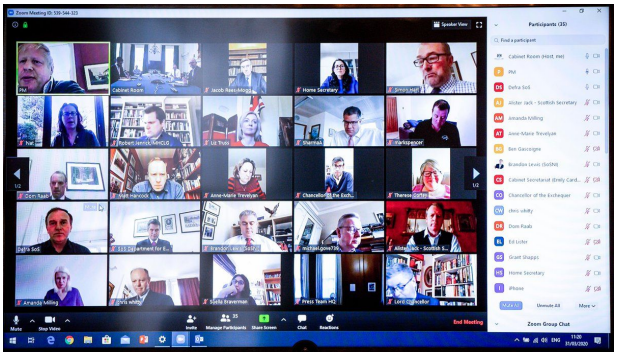
31 Rothschild Blvd.Tel Aviv, 6578414
Office: +972-3-6444417 | info@konfidas.com | www.konfidas.com

תוכן עניינים

איומים, התקפות והתראות

FBI מפרסמת אזהרה מפני חדירה לשיחות ועידה בפלטפורמת ZOOM

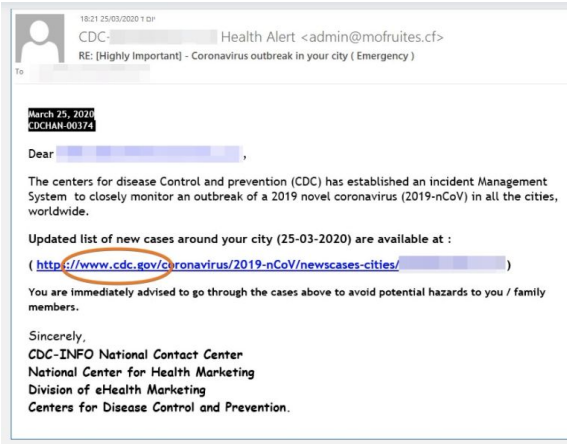
השימוש הגובר בפלטפורמת ZOOM מציבה אותה כמטרה לתוקפים. תקיפות אלו מכונות Zoom Bombing. ה-FBI מסר כי קיבל מספר דיווחים על כך ששיחות הועידה על גבי הפלטפורמה נקטעו בשל סרטונים פורנוגרפיים או תמונות שנאה שונות.[1]



צילום מסך של ועידת ZOOM בה נכח ראש ממשלת אנגליה חשף את פרטי הפגישה

בהמשך לאזהרת ה-FBI בנושא חשיפות של שיחות ZOOM, מופצת ברשת צילום מסך מתוך שיחת ZOOM שזה נמצא ראש ממשלת אנגליה. המשמעות היא שכל אחד יכול להקיש את מספר הזיהוי של השיחה ולנחש את סיסמת השיחה ובפשטות להיכנס לועידה.[2]

שלוש תקיפות דיוג (Phishing) חדשות הקשורות לקורונה


18:21 25/03/2020 יום ד'

CDC- Health Alert <admin@mofruites.cf>

RE: [Highly Important] - Coronavirus outbreak in your city (Emergency)

To

March 25, 2020
CDCHAN-00374

Dear ,

The centers for disease Control and prevention (CDC) has established an incident Management System to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in all the cities, worldwide.

Updated list of new cases around your city (25-03-2020) are available at :

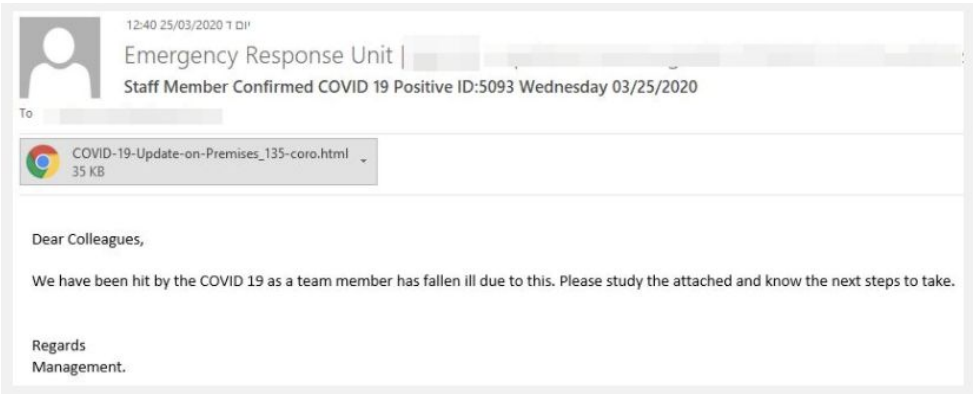
(https://www.cdc.gov/coronavirus/2019-nCoV/newscases-cities/)

You are immediately advised to go through the cases above to avoid potential hazards to you / family members.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease Control and Prevention.

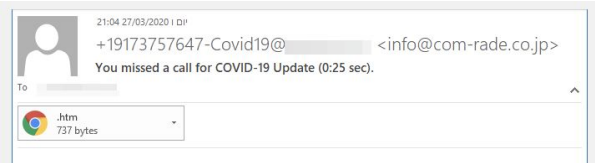
במאמר של חברת Perception Point מתוארות שלוש תקיפות דיוג (Phishing) מהימים האחרונים, אשר מטרתן גניבת נתוני הזדהות של משתמשים.[3] הקמפיין הראשון כולל שליחת דואר אלקטרוני המציין כי גורם מהארגון בו עובד הנמען נדבק בקורונה, ולכן הנמען מתבקש לפתוח קובץ מצורף, המכיל לכאורה הוראות וצעדים נדרשים לביצוע. בעת לחיצה על הצרופה נפתח עמוד התחברות מזויף, אליו הנמען נדרש להתחבר עם כתובת המייל והסיסמא הארגונית שלו. נתונים אלה נגנבים על ידי התוקפים.

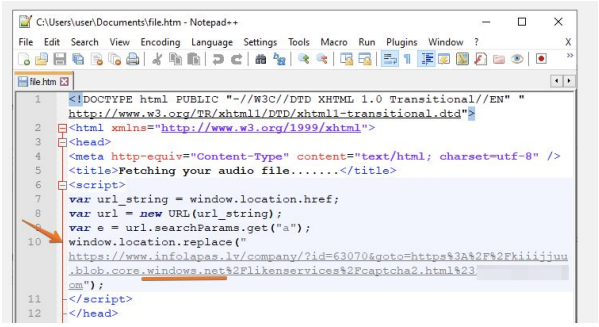
[1] FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic
[2] https://mobile.twitter.com/josephfcox/status/1245005703074336769
[3] https://perception-point.io/resources/incident-reports/covid-19-update-on-new-cyber-campaigns-3/



קמפיין הפישיג השני מכיל הודעה מזויפת מטעם המרכז לבקרת מחלות ומניעתן (CDC), אשר הקים מערכת לניהול אירועים וניטור התפרצויות של הנגיף. המייל מנחה את הנמען להיכנס לקישור לרשימת מקרי הידבקות מעודכנים באזור מגוריו, כדי לסייע לו, לכאורה, בהימנעות מהידבקות בנגיף הקורונה. למראית עין, הקישור למערכת שייך לדומיין לגיטימי: www.cdc.gov, אך למעשה מדובר בקישור זדוני המוביל לדף התחברות מזויף, אשר מאפשר גם הוא לתוקפים לגנוב את נתוני ההזדהות של המשתמש.

הקמפיין השלישי מכוון כלפי ארגונים המשתמשים בשירותים קוליים בשילוב עם התראות מייל. בקמפיין זה נשלח מייל מזויף שכותרתו: "שיחה שלא נענתה בנושא עדכון COVID-19", וקובץ htm מצורף. הקובץ מכיל קוד מסוג JavaScript המוביל לאתר פישינג, שמנסה לגנוב את נתוני ההזדהות של המשתמש.





סייבר וקורונה בישראל

משטרת ישראל מזהירה מפני ניסיונות סחיטה וירטואליים

על פי המשטרה, החשודים שולחים הודעה לפיה הקורבנות נראו צופים בתכנים מיניים, אולם לא מדובר באיום ממשי. בימים האחרונים התקבלו מספר תלונות במשטרת ישראל על דרישות כופר שהתקבלו באמצעות דואר אלקטרוני והודעות טקסט (SMS). בהודעות נכתב כי במכשיר של מקבל ההודעה הותקנה "תוכנה זדונית", והוא צולם כשביצע פעולות בזמן שצפה באתר המציג תכנים מיניים. מקבל ההודעה נדרש לשלם כופר בביטקוין כדי להימנע מהפצת אותם סרטונים. כדי להגביר את אמינות ההודעה, מצוין גם כי לתוקף יש שליטה מלאה על המכשיר של מקבל ההודעה.

מבדיקות המשטרה עולה כי מדובר בגורם זר, שלא מחזיק בחומר ממשי או בסרטונים כלשהם. הפרטים האישיים שלעיתים מצורפים להודעות אלו נלקחו מאתרים ישנים שנפרצו בעבר, ואין לסוחט פרטים אישיים נוספים של מקבלי ההודעות.[4]

פרקליטות המדינה שוקלת העמדה לדין בגין הפצת פייק ניוז

בציוץ הבא של ביני אשכנזי, נמסר כי מחלקת הסייבר בפרקליטות המדינה שוקלת העמדה לדין של תושב ראשון לציון, בגין שליחת הודעות פייק ניוז בשם משרד הבריאות.[5]

הפיקוח על הבנקים פרסם טיוטת עדכון בנושא מיקור חוץ

לאור ההנחיות לשעת חירום שנכנסו לתוקף בעקבות התפשטות מגפת הקורונה, דחה הפיקוח על הבנקים את מועד תחילת יישום הוראת ניהול בנקאי תקין מספר 359A בנושא מיקור חוץ, מ-20.3.31 ל-20.9.30.[6]

[4] https://www.gov.il/he/departments/news/police_31-3-20_virtual_extortion_warning
[5] https://twitter.com/BiniAshcknasy/status/1244982676630769664
[6] https://www.boi.org.il/he/BankingSupervision/DraftsFromTheSupervisorOfBanks/DocLib/111265.pdf

סייבר וקורונה בעולם

המלצות IT וסייבר לשדות התעופה בעקבות השיבושים שנגרמו ממגפת הקורונה

מועצת שדות התעופה הבינלאומית (ACI) פרסמה הנחיות IT וסייבר לשדות תעופה בעולם, בתגובה לשיבושים שנגרמו על ידי מגיפת COVID-19. מגבלות הטיסה והתנועה הובילו לירידה מהירה בכמות הנוסעים ועובדי שדות התעופה. הנחיות למניעת התפשטות המגפה אילצו שדות תעופה רבים לעבור לעבודה מרחוק, דבר המגדיל את הסיכון למתקפות סייבר. ההמלצות עוסקות בהגנת סייבר, בניית צוות ניהול משבר, המשכיות IT עם דגש לעבודה מרחוק ושיתוף מידע[7].

סוכנות האיחוד האירופי לאבטחת מידע פרסמה טיפים למשתמשים הרוכשים מוצרים באמצעות האינטרנט

בעקבות עלייה משמעותית של צרכנות באמצעות האינטרנט, סוכנות האיחוד האירופי לאבטחת מידע פרסמה טיפים לקנייה בטוחה של מוצרים אונליין. עיקרי הטיפים הינם: לוודא כי באתר הרכישה קיימת תעבורת מידע מוצפנת (יופיע סימן של מנעול לצד חלונית ה -URL), לבדוק באופן תדיר את הוצאות האשראי כדי לזהות העברות חשודות, לעדכן את מערכות ההפעלה של המכשיר עמו ניגשים לאתרי הקניות, ולשמור על הפרטיות האישית באמצעות הגדרת סיסמא חזקה והימנעות משיתוף מידע אישי עם גורמים לא מוכרים.[8]

שיח נרחב על הקורונה בדארקנט, הכולל תכנונים למתקפות פישינג

חברת Sixgill הישראלית הפיצה דו"ח בו היא סוקרת את הדיונים הקשורים לקורונה ברחבי ה- Darknet. הדיונים עוסקים בשיטות למינוף מצב הקורונה כדי להרוויח כספים באמצעות מתקפות דיוג (phishing), ובמכירת כלי נשק לקראת יום הדין. כמו כן, מדווח כי הגורמים הזדוניים נוטים להשתמש בהנדסה חברתית כדי לפרוץ למשתמשים.[9]

לפי דוח של פאלו אלטו: עלייה בפישינג, אפליקציות ודומיינים זדוניים

צוות ה-threat intelligence של חברת Palo Alto הנקרא Unit42, פרסם טרנדים הקשורים לקורונה המזוהים לאחרונה. הצוות דיווח על שלושה טרנדים עיקריים: א. מיילים של פישינג עם נוזקות המגיעים עם כותרות הקשורות לקורונה, ועם תוכן המשדר דחיפות ומיידיות, ב. אפליקציות אנדרואיד זדוניות אשר מתחזות לנותנות שירות הקשור בקורונה, ג. עלייה חדה בכמות הדומיינים הזדוניים ששמם קשור לקורונה.[10]

שיא בארה"ב: עלייה של 212% בשיחות אינטרנטיות ושימוש ב-VPN

חברת Comcast מציינת בדוח שלה שקיימת עליה של 212% בשיחות קוליות דרך האינטרנט (VoIP) ובשימוש ב-VPN. יתרה מזאת, החברה מדווחת על גידול של 32% בתעבורה בזמני שיא, ועל עלייה משמעותית בכל הנוגע לצריכת בידור, כולל שירותי סטרימינג והורדת משחקים.[11]

[7] https://aci.aero/news/2020/03/30/aci-issues-airport-it-best-practice-guidance-during-covid-19-pandemic/
[8] https://www.enisa.europa.eu/news/enisa-news/tips-for-cybersecurity-when-buying-and-selling-online
[9] https://info.cybersixgill.com/coronavirus-discourse-report
[10] https://www.ameinfo.com/industry/technology/unit-42-threat-brief-covid-19-cyber-victims
[11] https://corporate.comcast.com/covid-19/network

פתרונות

SANS מפרסמת עלון מודעות לניהול סיסמאות

אחד הפתרונות לעיבוי מערך ההגנה של כל משתמש הוא בחירת סיסמאות חזקות. כידוע, סיסמא חזקה צריכה להכיל כמות מסוימת של אותיות, תווים וספרות, מה שעלול להקשות על זכירת הסיסמה. על כן הפתרון המוצע הוא מנהל סיסמאות. לבחירת מנהל סיסמאות סאנס מציעה מספר טיפים: שימוש במנהלי סיסמאות אמינים וידועים, הימנעות משימוש במנהל סיסמאות אשר יכול לשחזר את סיסמת האב שלך (הסיסמה למנהל הסיסמאות עצמו), ועדכון גרסה של מנהל הסיסמאות באופן שוטף, על מנת להימנע מפרצות אבטחה.[12]

העשרה

עשרות אירועים וירטואלים בחינם של IEEE

תהנו![13]

[12] https://www.sans.org/sites/default/files/2020-03/202004-OUCH-Hebrew.pdf
[13] https://innovationatwork.ieee.org/events/virtual-events/

הציטוט היומי

"זום, הצליל שנשמע כאשר הפרטיות שלך עפה דרך החלון"[14]

(רונה סדנביק)

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 ***

[14] https://twitter.com/runasand/status/1245051108562735107