חדשות סייבר ונגיף הקורונה (COVID-19)

עדכון יומי ליום ג', 24.03.2020

הדוח מתפרסם גם במדור
"קפטן אינטרנט" של עיתון הארץ

הדוח מתפרסם גם בסייברנט

עיקרי הדברים

1. הפרקליט הראשי בניו-יורק פועל להגבלת הדומיינים המזויפים המנצלים את נגיף הקורונה
2. מתקפת סייבר על רשות בתי החולים בפריז
3. האקרים פורצים לנתבים ביתיים על מנת להפיץ פוגען לגניבת מידע
4. הרשות להגנת הפרטיות מחדדת את הצורך בשמירה על הפרטיות בעקבות התפשטות נגיף הקורונה

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

תוכן עניינים

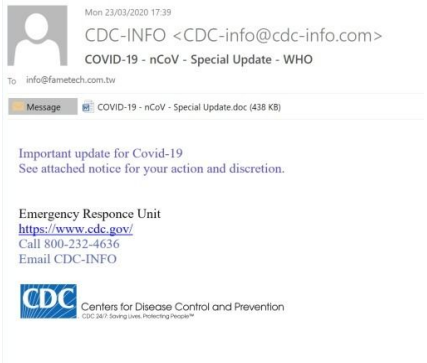
31 Rothschild Blvd.Tel Aviv, 6578414

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

איומים, התקפות והתראות

מתקפת סייבר על רשות בתי החולים בפריז

מטרת מתקפת הסייבר על רשות בתי החולים בעיר פריז הייתה להשבית את שירותי בית החולים על ידי גרימת עומסים גבוהים על מערכות המחשבים שלהם (DDoS). על פי דיווחים של רשות הגנת הסייבר הצרפתית (ANSSI), ההתמודדות עם המתקפה הייתה מוצלחת, ונזקים לא נגרמו בפועל. עוד מדווחת הרשות כי לא היו עד כה מתקפות סייבר נוספות הקשורות בנגיף הקורונה בצרפת.[1]


Mon 23/03/2020 17:39
CDC-INFO <CDC-info@cdc-info.com>
COVID-19 - nCoV - Special Update - WHO
To info@fametech.com.tw
Message COVID-19 - nCoV - Special Update.doc (438 KB)
Important update for Covid-19
See attached notice for your action and discretion.
Emergency Responce Unit
https://www.cdc.gov/
Call 800-232-4636
Email CDC-INFO
CDC Centers for Disease Control and Prevention

מייל פישינג נוסף המתחזה למרכז לבקרה ומניעת מחלות (CDC)

אנדרו קוסטיס, חוקר סייבר מומחה, מדווח על הודעת מייל מזויפת שנשלחה כביכול מטעם ה-CDC. בתוך הודעת המייל יש מסמך מצורף מסוג doc אשר מכיל בתוכו קטע הרצה זדוני (http://getegroup[.]com/file.ex), ומשתיל פוגען אשר גונב מידע מהמחשב הנתקף.[2]

אנטי-וירוס מזויף משמש למתקפות סייבר הקשורות לנגיף הקורונה

נמצא אתר נוסף המנצל את בהלת הקורונה, והפעם האתר מפרסם תוכנה מזויפת המשווקת אנטי-וירוס לכאורה חדשני, וייעודי להגנה מפני מתקפות סייבר הקשורות לקורונה: "antivirus-covid19[.]site". דרך הפעולה שלו היא ניצול מחשבים מותקפים כדי ליצור רשת מחשבים עליה שולט התוקף, על מנת ליצור מתקפות רחבות היקף. משתמשים שמורידים את התוכנה המזויפת נופלים קורבן לפוגען BlackNet, מסוג Remote Access Administration (RAT).[3]

האקרים פורצים לנתבים ביתיים על מנת להפיץ פוגען לגניבת מידע

במודל חדש של מתקפות סייבר, האקרים פורצים לנתבים ביתיים, משנים את הגדרות ה-DNS (Domain Name System) בנתבים, ומציגים התראות מטעם ארגון הבריאות העולמי (WHO). בהתראות אלה ישנו קישור להורדת אפליקציה זדונית, המכילה תוכנה לגניבת מידע (COVID-19 Inform App). הפוגען שמוטמע בתוכנה אוסף היסטוריית גלישה, פרטי תשלום, ארנקים קריפטוגרפיים ועוד.[4]

עדכון מזהים של אתרים חשודים

חברת X-Force הוסיפה מזהים (IOCs) חדשים של פוגענים עדכניים ל-24.03.2020 . מומלץ להיכנס ללינק המצורף ולהזין את כלל המזהים במערכות ההגנה שלכם. גם ב-X-Force ניתן למצוא רשימה של דומיינים חדשים הקשורים

[1] https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says
[2] https://app.slack.com/client/TVD5F8P0B/C010A5TAK1A/thread/C010A5TAK1A-1585049332.478400
[3] https://blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool/
[4] https://www.bleepingcomputer.com/news/security/hackers-hijack-routers-dns-to-spread-malicious-covid-19-apps/

לקורונה, חלקם אף עדיין אינם פעילים אך צפויים להיות בעתיד. לדוגמא: coronaviruscovid19-informationp[.]com, googlecoronavieus[.]com, coronavirus-status.s3.eu-central-1.amazonaws[.]com ועוד רבים.[5] [6]

קבוצת תקיפה TA505 מטרגטת עובדי משאבי אנוש בגרמניה

במבצע התקיפה, הקבוצה שולחת הודעות מייל למחלקת משאבי אנוש, כאשר בגוף ההודעה יש קובץ מצורף עם קורות חיים של "מועמדים לעבודה". עם פתיחת הקובץ נפתחות לתוקף יכולות לגנוב מידע, לגנוב פרטי משתמש ולהצפין את המידע במחשב הנתקף. כרגע תקיפה זו מכוונת לחברות בגרמניה, אך אין המונע מהם להתפשט לחברות בעולם כולו.[7]

פולין פרסמה אפליקציה שמאלצת חולי קורונה לצלם תמונות סלפי לצורך הוכחת בידוד

האפליקציה "Home Quarantine" נוצרה על מנת לוודא כי אנשים אשר צריכים להיות בבידוד אכן נשארים שם. בעת ההרשמה מבצעים סלפי לצורך השוואה, האפליקציה מקפיצה התראות על צילום תמונות בזמנים אקראיים ומשווה אותם למיקום של החולים על מנת לוודא שהם נמצאים עדיין במקום הבידוד. האפליקציה היא אופציה לבחירת החולה מתוך שתיים, השנייה היא ביקורי פתע של שוטרים.[8]

סייבר וקורונה בישראל

הרשות להגנת הפרטיות מחדדת את הצורך בשמירה על הפרטיות בעקבות התפשטות נגיף הקורונה

הרשות להגנת הפרטיות פרסמה מסמך המדגיש את החשיבות של שמירה על פרטיות והגנה על מידע אישי, בהמשך לכניסה לתוקף של התקנות לשעת חירום, המאפשרות (בין השאר) איסוף מידע אישי ועיבודו לצורך התמודדות עם נגיף הקורונה. המסמך מתייחס לשאלות ותשובות רלוונטיות למצב הנוכחי. לדוגמה: "איך אפשר להגן על מידע אישי של עובדים/סטודנטים/תלמידים הפועלים מרחוק?" במסמך, הרשות מציינת כי "...עמדת הרשות להגנת הפרטיות היא כי גם במצבי חירום, כאשר קיימת הצדקה לכאורה לפגיעה בפרטיות כלל הציבור או חלקים ממנו, יש להקפיד לפעול בהתאם לעקרונות ההגנה על פרטיות, ועל כך שהפגיעה הנגרמת כתוצאה מהפעילות לא חורגת מהנדרש בנסיבות העניין."[9]

[5] https://exchange.xforce.ibmcloud.com/collection/CoronaVirus-Themed-Domain-161988a5dd11ee521755f4880bac18a5

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

[7] https://blog.prevailion.com/

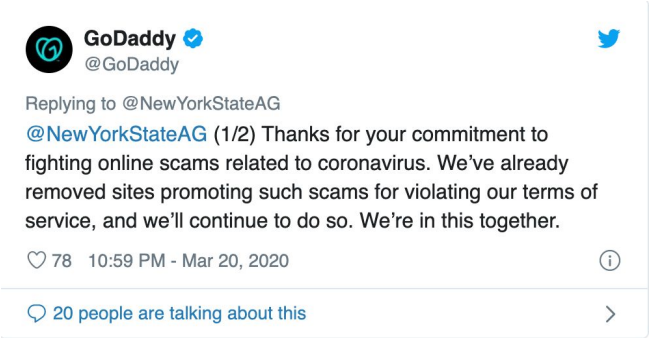
[8] https://www.france24.com/en/20200320-selfie-app-to-keep-track-of-quarantined-poles

[9] https://www.gov.il/BlobFolder/reports/korona_privacy/he/PRIVACY_CORONA_QA.pdf

סייבר וקורונה בעולם

הפרקליט הראשי של ניו יורק פועל להגבלת דומיינים מזויפים המנצלים את נגיף הקורונה

משרד הפרקליט הראשי של ניו-יורק הגיש מכתב[10] לשש החברות הגדולות המוסמכות כרשמות (Registrar) של שמות מתחם בארה"ב. המכתב דורש לבחון מספר הגבלות על תהליך המכירה של שם דומיין, בין ההגבלות: בחינה אוטומטית וידנית של דומיינים חדשים הקשורים בוירוס הקורונה, מניעה של שימוש בדומיינים שדווחו כמזויפים ועוד. נראה כי התגובות של החברות הן חיוביות והן אכן נרתמות למאבק.[11]



טוויטר מעדכנת את תחזיות הרווח ל-Q1 עקב שינויים בעקבות הקורונה

מגפת הקורונה לא פוסחת גם על טוויטר, אשר נאלצת לבצע הערכת מצב מחודשת של צפי הרווחים של החברה, בהתאם לשינויים החלים במשק. החברה צופה כי הכנסות הרבעון הראשון יירדו מעט וגם להפסד הפסד תפעולי..[12]

דיווח שגוי על מתקפת DDOS נגד האתר הממשלתי MyGov של אוסטרליה

בתחילת השבוע הכפיל הממשל האוסטרלי את ההטבות למובטלים בעקבות השלכות נגיף הקורונה על המשק. באזור השעה 09:00 האתר "MyGov" קרס ולא היה זמין להמוני גולשים. שר השירותים האוסטרלי הצהיר כי האתר עבר מתקפת DDOS, אך מספר שעות לאחר מכן חזר בו מהצהרתו כאשר התברר כי האתר קרס בעקבות פניות רבות של אלפי תושבים אוסטרליים, וכי מערכות הניתוח דיווחו התראת שווא. [13]

[10] http://www.documentcloud.org/documents/6817833-NY-AG-Letter-Concerning-Godaddy-and-Coronavirus.html
[11] https://twitter.com/GoDaddy/status/1241107127709597696?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1241107127709597696&ref_url=https%3A%2F%2Fwww.zdnet.com%2Farticle%2Fnew-york-asks-domain-registrars-to-crack-down-on-sites-used-for-coronavirus-scams%2F
[12] https://investor.twitterinc.com/files/doc_news/2020/03/TWTR-Withdraws-Guidance-Announcement.pdf
[13] https://www.theguardian.com/australia-news/2020/mar/23/incompetence-attack-mygov-website-did-not-crash-because-of-ddos-cyber-assault-as-stuart-robert-claimed

פתרונות

חב' מקינזי מפרסמים 8 טיפים לעבודה מרחוק, על בסיס צבירת ניסיון של החברה בסין

המדינה הראשונה שספגה את השלכות הקורונה הייתה סין, ומכאן שהיא גם צברה את הניסיון הרב ביותר בהתמודדות עם המצב. בדו"ח של מקינזי, משולבות עצות שנובעות מלמידה אחר הנעשה בסין, והתמודדותה עם עבודה מרחוק. מבין העצות שניתנו: יצירת מבנה ברור של צוותי העבודה, על מנת למנוע מצבים של חוסר וודאות ובלבול אשר יוצרים פיזור פתאומי של העובדים, הבנה ארגונית כי אכן מדובר בתקופה קשה ומלחיצה כלפי מבחינת העובדים, וגילוי אמפתיה במצבים רגישים אלה.[14]

מתנדבים שעוזרים למוסדות רפואיים להתגונן מפני מתקפות סייבר

Cyber Volunteers 19 הם קבוצת מומחים באבטחת מידע אשר מתנדבים לתת מענה הגנתי לתקיפות הסייבר המרובות כנגד מוסדות רפואיים. במהלך השבוע האחרון הצטרפו 3000 מתנדבים חדשים לקבוצה, מכל העולם, על מנת לתרום למאמץ. הקבוצה הוקמה על מנת לסייע למוסדות רפואיים לזהות, להגן ולהגיב לאיומי סייבר.[15]

ערוץ Slack לשיתוף איומי סייבר הקשורים לנגיף הקורונה

בערוץ נמצאים חוקרי סייבר שמפרסמים התראות על הודעות פישינג, פוגענים חדשים ואת המזהים שלהם, לצורך הכנסתם למערכות ההגנה[16].

העשרה

ה-NCCoE פרסם טיוטה של מסמך NIST העוסק בהגנת נכסים מפני מתקפות כופר ואירועים חמורים

המסמך מציג את ההשלכות שיש למתקפות כמו כופרה, פוגענים הרסניים, איומים פנימיים על תשתית הארגון, המידע והלקוחות שלו. מתוך כך ריכזו פעולות שיש לעשות כדי לזהות נכסים מהותיים שעלולים להוות מטרה למתקפות סייבר שונות. במסמך יש גם התייחסות לאמצעי הגנה שיש להטמיע כדי להתמודד עם מתקפות שונות.[17]

מכללת See Security מציעה קורס מקוון חינמי

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.[18]

[14] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/a-blueprint-for-remote-working-lessons-from-china?cid=other-eml-alt-mip-mck&hlkid=71a1ebea808e42f9a82e0716ac7ffae8&hctky=9325559&hdpid=8a7d725d-49e2-4b4e-91f7-ff6a4dadb4b5

[15] https://cyberv19.org.uk/

[16] https://app.slack.com/client/TVD5F8P0B

[17] https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect

[18] https://www.see-security.com/%d7%a7%d7%95%d7%a8%d7%a1%d7%99%d7%9d/%d7%9e%d7%aa%d7%97%d7%99%d7%9c%d7%99%d7%9d-%d7%91%d7%9e%d7%97%d7%a9%d7%91%d7%99%d7%9d-%d7%95%d7%94%d7%a9%d7%9c%d7%9e%d7%95%d7%aa/free-course-by-cisco-introduction-to-cyber-security/

הציטוט היומי

"הערב, בהתאם להנחיות האחרונות של ה-CDC וכדי למנוע התאספות של יותר מ-10 אנשים, אני מדבר איתכם מביתי בוילמינגטון, דלוור."

ג'ו ביידן,

מועמד מוביל של המפלגה הדמוקרטי לנשיאות של ארה"ב, על התופעה החדשה של CFH - Campaigning from Home - הצורך לנהל קמפיין מקוון בגלל התפשטות וירוס הקורונה.[19]

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 ***

[19] https://www.wsj.com/articles/joe-biden-looks-to-build-digital-capabilities-amid-pandemic-11584964800