

מידע רדיו וטלוויזיה

IFAT House

96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת

דרך מנחם בגין 96-98, תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

לינק לקובץ: [לחץ כאן](#)

תוכנית: שלושה שיודעים

תאריך: 18/08/2024

שעה: 08:23:24

רשת: כאן תרבות



כותרת: ד"ר שרה ביתן, חוקרת בכירה במרכז המחקר לאבטחת סייבר בטכניון ומנכ"לית

נתיב רובינזון : כאן תרבות, שלושה שיודעים. עכשיו אנחנו עם קצת חדשות סייבר. צוות מחקר מהטכניון שימו לב, הצליח להשתלט על בקר של חברת סימנס. מדובר באחד הבקרים המאובטחים בעולם שמשמש מערכות כמו רמזורים, כלי טיס, אפילו כורים גרעיניים. האם אנחנו אמורים להילחץ מזה או שזה פועל לטובתנו? נאמר בוקר טוב לדוקטור שרה ביתן, חוקרת בכירה במרכז המחקר לאבטחת סייבר בטכניון, מנכ"לית חברת סייקלוק שמספקת ייעוץ בנושא אבטחת סייבר. בוקר טוב, שרה.

ד"ר שרה ביתן : בוקר טוב, נתיב.

נתיב רובינזון : אז את יודעת, ישר אנחנו באמת, זה טוב לנו או שזה רע לנו? זה מלחיץ אותנו או שדווקא זה צריך להרגיע אותנו? כי אם הצלחתם לעשות את זה, זה אומר שעכשיו יידעו מה לעשות הלאה?

מידע רדיו וטלוויזיה

IFAT House

96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת

דרך מנחם בגין 96-98, תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

ד"ר שרה ביתן : בגדול, זה צריך להרגיע אותנו.
נתיב רובינזון : הו, נרגעתי, תודה רבה. אני רוצה לאחל לך בוקר טוב ולהודות לך שהיית איתנו היום בתוכנית, אוקיי. אז אנחנו נרגעים. כן. אז בואי תרגיעי אותנו, כן.
ד"ר שרה ביתן : כן, אוקיי. טוב, אז בואו נתחיל ראשית כל במה זה הבקרים התעשייתיים האלה. אז למעשה זה מחשבים מיוחדים ששולטים ומנטרים בתהליכים בעולם הפיזי. לדוגמה, אתה יכול להריץ על בקר כזה תוכנית שמודדת לחץ בדוד קיטור, ופותחת שסתום במקרה שהלחץ גבוה מדי, או תוכנית שמודדת את רמת הכלור במים, ומורה לעצור או להמשיך את ההזרמה של הכלור בהתאם לרמה. עכשיו, כולנו מבינים שווירוס יכול לגנוב את סיסמת ה-X שלנו, הטוויטר ולכתוב פוסט בשמנו או לגנוב את סיסמת הבנק שלנו ולמשוך כספים, אבל וירוס שמשתלט על בקר כזה, בקר תעשייתי, יכול לשבש את קריאת מד הלחץ ולגרום חס וחלילה לפיצוץ או להזרים כמות גדולה של כלור למים, ולגרום להרעלה.
נתיב רובינזון : אגב, למה אנחנו, למה אנחנו אומרים שסימנס הוא נחשב הקרם דה לה קרם של החבר'ה האלה? בבקרים המאובטחים?
ד"ר שרה ביתן : אז סימנס שהיא חברה גרמנית, היא די השליטה בסוג של הבקרים התעשייתיים. זאת אומרת, מירב הבקרים

מידע רדיו וטלוויזיה

IFAT House

96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת

דרך מנחם בגין 96-98, תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

שתמצא ברשתות של חברות חשמל, חברות רכבות, תאגידי מים, הם בקרים של סימנס. עכשיו, התקיפה הראשונה, המאוד מפורסמת שבעצם הבהירה לנו שאנחנו יכולים על ידי וירוס מחשבים לגרום לאיזושהי תופעה בעולם הפיזי, הייתה, התגלתה בשנת 2010, היא תקיפה של וירוס מחשבים שנקרא סטאקס נט.. הווירוס הזה תקף בכור הגרעיני האיראני בנתנז, וגרם לכך ש.. נתיב רובינזון : שזה דווקא טוב.

ד"ר שרה ביתן : נכון.

נתיב רובינזון : כן.

ד"ר שרה ביתן : מבחינתנו כן.

נתיב רובינזון : נכון.

ד"ר שרה ביתן : ובעצם הוא גרם לכך שצנטריפוגות שנועדו להעשרת אורניום, הסתובבו במהירות גבוהה מדי, וכתוצאה מכך, אחרי מספר חודשים הם נסדקו ויצאו מכלל פעולה, ועל פי מקורות זרים, זה גרם לעיכוב של כמעט שנה בתהליך העשרת האורניום של איראן. עכשיו הווירוס הזה, תקף בקרים של סימנס. בעצם מה שהוא עשה, הוא מצד אחד, הגביר את המהירות של הצנטריפוגות, ומצד שני, לרכיב שמנטר, הוא אמר, הכל בסדר, הצנטריפוגות מסתובבות במהירות הרגילה, לא צריך להיבהל. עכשיו, כתוצאה מזה ש..

נתיב רובינזון : כלומר, על משקל הרצחת וגם ירשת, פה זה

מידע רדיו וטלוויזיה

IFAT House

96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת

דרך מנחם בגין 96-98, תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

הרצחת וגם הרגעת אותם שלא קרה כלום. זאת אומרת, הם..

ד"ר שרה ביתן : נכון.

נתיב רובינזון : חשבו שעוד הכל בסדר.

ד"ר שרה ביתן : בדיוק. עכשיו, כתוצאה מזה, סימנס באמת נכנסה

לפעולה והיא הייתה היצרן הראשון שהכניס רכיבי אבטחה

משמעותיים לתוך הבקרים שלו. מעשית מה שהם עשו, הם הכניסו

קריפטוגרפיה, הצפנה לפרוטוקולי תקשורת ש... אנחנו בעצם התחלנו

את המחקר שלנו מתישהו בשנת 2017, ובשנת 2019 פרסמנו בכנס

שנקרא בלאק הט, עבודה שתקפה את פרוטוקול התקשורת החדש

שלהם, ובעצם הראינו שאנחנו עדיין יכולים להזריק תוכנית שתגביר

את מהירות הצנטריפוגות וכך תשבש את הפעילות שלהם, וכתוצאה

מכך סימנס, בשילוב של מחקר שלנו ושל חברת קלארוטי שהיא

גם חברה ישראלית, בעצם סימנס שיפרו את פרוטוקול התקשורת,

והם יצאו בשנת 2020 עם פרוטוקול תקשורת משופר שמתמש

בפרוטוקול סטנדרטי בתעשייה.

נתיב רובינזון : שאלה חשובה, דוקטור ביתן ברשותך,

ד"ר שרה ביתן : כן.

נתיב רובינזון : כשאתם בעצם חוקרי הטכניון עושים מתקפה כזו

על הבקר, הרי זו מתקפה שמטרתה חיובית, מעדכנים מראש את

החבר'ה בסימנס שעושים את זה?

ד"ר שרה ביתן : כן. כן, אנחנו כבר,

מידע רדיו וטלוויזיה

IFAT House

96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת

דרך מנחם בגין 96-98, תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

נתיב רובינזון : כן?

ד"ר שרה ביתן : האמת היא די יש לנו קו חס לסימנס. אנחנו..
נתיב רובינזון : לא, אבל אתם אומרים להם, ביום זה וזה נעשה
מתקפה, או שרק אחר כך אתם אומרים להם, עשינו והנה תראו
את התוצאות?

ד"ר שרה ביתן : לא. אנחנו מבצעים את המתקפה במעבדות שלנו
בטכניון, בסביבה מבודדת שחשופה רק אלינו, זאת אומרת היא לא
חס וחלילה יכולה לדלוף לעולם החיצון. אחרי שאנחנו מוודאים
את תוצאות המתקפה ומוודאים שהיא באמת עובדת כמו שציפינו
שהיא תעבוד, אנחנו משתפים את סימנס עם כל פרטי המתקפה.
מעשית, יש לנו גם מחויבות בתור מה שנקרא וואייט האקס..
זאת אומרת חוקרי סייבר חיוביים, אנחנו מחויבים לתת לסימנס או
לכל יצרן, התראה של לפחות 90 יום לפני שאנחנו מפרסמים את
תוצאות המחקר שלנו, בכדי שתהיה להם הזדמנות לתקן.
נתיב רובינזון : כלומר, שולחים להם את התוצאות, נותנים להם
אפשרות להגיב לפני שאתם מפרסמים. זאת אומרת, הם מקבלים
את זה ראשונים לעיניהם בלבד.

ד"ר שרה ביתן : נכון, נכון. ובעצם כל המוטיבציה של המחקרים
האלו, בכלל של כל הקהילה הזאת שהיא וואייט האקר, זה א',
להביא למודעות של כולנו שהתקיפות האלה אפשריות בכדי שנהיה
מוכנים, וזה לשני חלקי הקהילה. ראשית כל, ליצרנים, סימנס,

מידע רדיו וטלוויזיה

IFAT House

96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת

דרך מנחם בגין 96-98, תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

אנחנו מראים להם, הנה, תראו מה אנחנו יכולים לעשות, בבקשה
תתכבדו ותתקנו את זה. ומצד שני, ללקוחות אנחנו אומרים, תדעו
לכם, היכולות תקיפה הן כאלה וכאלה, אתם צריכים להגן על
עצמכם וכאשר אתם רוכשים בקרים, לדרוש מהיצרן, בבקשה תיתנו
לנו הגנה נאותה לבקרים,
נתיב רובינזון : אז אנחנו..

ד"ר שרה ביתן : מכיוון שאם לא, אנחנו חשופים.

נתיב רובינזון : אז אנחנו באירוע הזה, זאת אומרת, זה תרתי
משמע, המושג אור לגויים, כלומר, סימנס עם כל הכבוד, בסוף
מגיעים מה שנקרא, חברינו מהטכניון, ומתגברים על כל הגאונות
של סימנס.

ד"ר שרה ביתן : כן, נכון. במקרה הזה, זה מדויק.

נתיב רובינזון : את יכולה להסמיק, זה בסדר, לא, לא, לא, לא,
זה שלכם, זה הצוות שלכם. אז זה מדהים, זאת אומרת, בשורה
התחתונה, סימנס כמו שאמרנו, שהם הקרם דה לה קרם בעניין
של ההצפנות, בסוף יושבים אנשים רציניים בטכניון ופורצים את
זה.

ד"ר שרה ביתן : נכון.

נתיב רובינזון : אז בשורה התחתונה זה כן קצת מדאיג, זאת
אומרת..

ד"ר שרה ביתן : תראה, אתה יכול לטמון את ראשך, א', דבר

מידע רדיו וטלוויזיה

IFAT House

96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת

דרך מנחם בגין 96-98, תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

אחד שצריך להגיד, מאז סטאקס נט כמעט ואין תקיפות כאלה שמכוונות לבקרים תעשייתיים. זאת אומרת, בניגוד להתקפות בעולם הווירטואלי שקורית כל שני וחמישי, תקיפות על בקרים תעשייתיים הם יחסית יותר נדירות. עכשיו, בנוסף, הרשתות האלה כפי שכמובן אנחנו צריכים להבין, הם מוגנות היטב. ברובן... בכלל לא מחוברות לרשתות חיצוניות ומאוד קשה לחדור אליהם. עם זאת, אנחנו דורשים שהאבטחה בתוכם תהיה זה ברמה מאוד גבוהה. אז ראשית כל, ההתקפות האלה הן עוד לא נפוצות, ושנית, העבודה שלנו באמת עושה שינוי. עובדה, כתוצאה מהמחקר שפרסמנו ב-2019, סימנס תיקנו את פרוטוקול התקשורת וגם עכשיו אני מאמינה שכתגובה למה שאנחנו פרסמנו, הם ישפרו את האבטחה. זאת אומרת, לתוקפים, יש, העובדה שהם לא מפרסמים את התוצאות שלהם לא אומרת שאין להם ידע.

נתיב רובינזון : כן.

ד"ר שרה ביתן : לכן, אנחנו מבחינת התעשייה צריכים כל הזמן להיות מודעים לסכנות, בכדי שנמשיך ונתקן אותם. נתיב רובינזון : מי עוד ככה ברחבי העולם, קולגות שלכם שעושים את התקיפות הללו? זאת אומרת, מדענים מה שנקרא מקבילים לכם ממדינות אחרות גם הם ככה תוקפים את סימנס, פרום טיים טו טיים?

ד"ר שרה ביתן : כן, כן. יש חברה גרמנית שפרסמה תוצאות בכנס

מידע רדיו וטלוויזיה

IFAT House

96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת

דרך מנחם בגין 96-98, תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

הקודם בבלאק הט בלונדון, יש מכון מחקר בשווייץ שפרסם תוצאות גם על סדרה אחרת של בקרים של סימנס. יש לא מעט מכוני מחקר שמתעסקים בנושא של אבטחת בקרים תעשייתיים. נתיב רובינזון : אז הנה כך למדנו. אגב, זה אולי לא קשור לעניין שלנו, סימנס היא כמובן חברה הנסחרת בבורסה, זה משפיע גם על דברים כאלה כשמתפרסמים דברים מן הסוג הזה? אני מתקיל אותך במשהו שלא קשור אלייך, סתם פשוט, זה פתאום עלה לי אסוציאטיבית.

ד"ר שרה ביתן : .. כן. אז תראה, תקיפה בעולם האמיתי כן, חולשות בדרך כלל ההשפעה שלהן היא, זאת אומרת, תקיפות כמו שלנו, ההשפעה שלהם היא יותר מינורית, זה בעצם מצומצם לקהיליית הסייבר, וסימנס באמת נותנים מענים. נתיב רובינזון : כן.

ד"ר שרה ביתן : אז זה לא, אני לא מאמינה, לא בדקתי את המניה של סימנס, אבל אני לא מאמינה שזה מגיע עד לשם. נתיב רובינזון : טוב.. לא, התקלתי אותך פשוט, אז אני אומר, אסוציאטיבית פתאום נזכרתי, הם נסחרים בבורסה, אז יכול להיות.. אז הנה כך, החברים בסימנס, שמקבלים עזרה מהחברים בטכניון. נזכיר את החברים, נכון? נדב אדיר, אלון דנקנר, פרופסור אלי ביהם, נכון? הזכרתי את כולם, וכמובן אותך, דוקטור שרה ביתן, נכון?

מידע רדיו וטלוויזיה

IFAT House

96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת

דרך מנחם בגין 96-98, תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

ד"ר שרה ביתן : ואור קרת ורון פרודנטל שגם שותפים במאמר
ובמחקר כמובן.
נתיב רובינזון : אז הנה, דוקטור שרה ביתן, חוקרת בכירה במרכז
המחקר לאבטחת סייבר בטכניון, מנכ"לית חברת סייקלוק שמשפיקת
ייעוץ בנושא אבטחת סייבר, אנחנו רוצים מאוד-מאוד להודות לך
על השיחה הזו. גם הרגעת אותנו, גם הדאגת אותנו והרגעת אותנו
עוד פעם, זאת אומרת זה מין סנדוויץ' כזה שסגר את השיחה
ואנחנו יוצאים רגועים, תודה רבה.
ד"ר שרה ביתן : תודה רבה לך, נתיב. יום טוב.