

ניסיון סחיטה במייל כופר עכשיו גם בעברית

"התרשמתי מאוד מאתרי התוכן האינטימיים שבהם אתה מבקר מדי פעם", כך נכתב במייל שנשלח לישראלים וישראליות בחודש האחרון. העבריינים דורשים תשלום בביטקוין ומאיימים כי אם הקורבנות לא ישלמו הם ישלחו לרשימת אנשי הקשר שלהם במייל וברשתות החברתיות הקלטה של התוכן הפורנוגרפי בו צפו. לאחרונה זיהינו קמפיין הונאה במהלך אמצע חודש אוקטובר (16-18.10). הקורבנות הישראלים קיבלו מייל הטוען כי הושלל וירוס טרויאני במחשבם והתוקפים תיעדו את התוכן הפורנוגרפי בו הם צפו. בהמשך המכתב מאיימים על הקורבן בפרסום התוכן המיני בו צפה במחשב בתפוצה לכל אנשי הקשר שלו במייל וברשתות החברתיות במידה ולא יעביר סכום כסף בביטקוין לארנק הדיגיטלי של התוקפים.

התופעה היא לא חדשה, מיילים מהסוג הזה [התגלו כבר בחודש יולי האחרון](#), אך אם עד היום המיילים התקבלו באנגלית, בחודש האחרון אנו מדווחים על כך שעברייני הרשת נעזרים בשירות תרגום בסיסי על מנת לטרגט ישראלים.

בפועל מדובר בהונאה ומשטרת ישראל מבהירה כי לשולחים אין סרטונים של הנסחטים. במהלך החודשים האחרונים התקבלו אצלנו עשרות פניות מלקוחות ושותפים שלנו שקיבלו מכתב כופר במייל ובו דרישה לתשלום בביטקוין תמורת אי פרסום מידע מפליל על הקורבן. בקמפיין האחרון שזיהינו, תרגמו בפעם הראשונה את הודעת האיום לעברית, כאשר הקמפיין ארך 3 ימים במהלכם ראינו שחלק מהקורבנות אכן העבירו סכום של \$300 לתוקפים".

על מנת לשוות מראה אמין למתקפה בגלים הקודמים צורפה סיסמה של החשבון ובגל הנוכחי נראה שנשלח המייל מכתובת המייל של הקורבן, כאשר כביכול לתוקף גישה לתיבת המייל והוא שלח ממנה. בפועל ניתן בקלות לזייף את כתובת השולח, וכך גם במקרה זה.

על אף שגיאות הכתיב ובעיות התחביר כנראה שהשליחה מכתובת הנמען גרמה לכמה קורבנות להשתכנע ולשלם את הכופר. כך כבר 6 קורבנות ששילמו את סכום הכופר שדרשו התוקפים. ניתן גם לראות שלאחר סיום ה"קמפיין" שארך 3 ימים, משכו העבריינים סכום של \$1,500 ששולמו בביטקוין מהארנק הדיגיטלי שנפתח במיוחד עבור התקיפה.

ההמלצה שלנו היא לא לענות או להתייחס להודעות מסוג זה ולהגיש תלונה במשטרה במידה וקיבלתם מייל בסגנון הזה. בנוסף, חשוב מאוד להחליף את הסיסמאות לשירותים השונים, במיוחד אם נעשה שימוש חוזר באותה הסיסמה עבור מספר חשבונות. ניתן ומומלץ לבדוק האם [כתובת המייל נמצאת כאן](#) כדי לבדוק אם היא נמצאת במאגרי סיסמאות שדלפו.

פרטיות המידע תקיף ותפיל חברות

מכיוון שמתקפות סייבר, דליפות מידע ותקלות פרטיות הפכו לפולשניות ומזיקות באופן חסר תקדים, גופים רבים יותר ירצו לדאוג לבטיחותם של הנכסים הדיגיטליים שלנו. זה יוביל לכך שהגישות המובילות להגנה על אבטחת המידע יתמקדו בהגנה על מערכות הממוחשבות והנתונים הממוחשבים של כולנו. אם ישנו קו מנחה אחד שמשיק לכל הנושאים במאמר הזה, הוא יהיה ההתמקדות [בהגנה על המידע ופרטיותו](#).

דוח המגמות של ESET לשנת 2019 נוגע בנושא האחריות של ענקיות טכנולוגיה, כמו גוגל ופייסבוק, בכל מה שקשור להגנה על כמות הענק של הנתונים שצברו על המשתמשים שלהן במהלך השנים. מכיוון שאנחנו מסתמכים על שירותיהן של השתיים על בסיס יומיומי בכל דבר שנוגע לחיים המקוונים שלנו, אנו שואלים אם אנחנו מניחים את כל הביצים באחד מהסלים האלה (או בשניהם), האם ייתכן מצב בו נמצא את עצמנו בבעיה אם הביצים נופלות מאחד מהם?

חוקרי ESET טוענים כי מקרים כמו תקרית קיימברידג' אנליטיקה עשויים לגרום לאנשים לחפש אלטרנטיבות לפלטפורמות ששולטות בשוק היום. מכיוון שאנשים פרטיים, חברות ועברייני רשת נותנים כולם חשיבות רבה לנתוני הלקוחות, הטענה המרכזית היא שיכולתה של חברה לשמור על פרטיות המידע שברשותה תקבע האם תוכל לשרוד בשנת 2019.

שימוש באוטומציה לקידום קמפינים של הנדסה חברתית

אנחנו מספרים לכם כאן מדי שבוע על מתקפות פשינג שבאמצעות הנדסה חברתית משומנת גורמים לנו להזין פרטים רגישים באתרים מזויפים המתחזים לשירותים לגיטימיים. אנחנו מעריכים שבשנת 2019 נראה עלייה בשימוש באוטומציה ובלמידת מכונה (Machine Learning) בקרב עברייני רשת, זאת על מנת לאסוף מידע רב יותר כדי להפעיל קמפיני הנדסה חברתית מתוחכמים ואישיים יותר. אמנם לא סביר שלעברייני הרשת תהיה גישה לכמות הנתונים העצומה שמאוחסנת ע"י יצרניות המכשירים, כמו סבבי הקניות הקבועים של המשתמשים, אך הם יוכלו ליצור פרופילים מדויקים יותר לכל אדם באמצעות שימוש ב Web Trackers-שעוקבים אחרי הקורבנות גם כשהם עוברים לאתר אחר, או איסוף מידע מגופים מיוחדים לניהול וסחר בנתונים.

התוקפים מכוונים למכשירי בית חכם

העלייה בתפוצתם של המטבעות הוירטואליים, יחד עם העלייה במספר המכשירים שמחוברים לאינטרנט, עשויה להוביל לכך שמכשירים חכמים והעוזרות החכמות יהפכו לפרצה שבאמצעותה עברייני רשת יבנו רשתות לכריית מטבעות וירטואליים בשנת 2019.

כבר ראינו כיצד עברייני רשת משתמשים במכשירי "אינטרנט של הדברים" (IoT) "כדי ליצור מתקפות מניעת שירות, (DDoS) וככל שיותר מכשירים יתחברו לאינטרנט ויהפכו לחלק מחייהם של אנשים בשנה הקרובה, כך גם התוקפים ימשיכו לחפש נקודות תורפה במכשירים וישתמשו בהם כדי לתקוף משתמשים רבים יותר. בעולם שמשווע לנוחיות באמצעות טכנולוגיה, אין תחליף לנוחיות שטמונה ביכולת שלנו ללכת לישון בזמן שהגאג'ט שלנו דואג לכבות את האור אחריו. אחרי הכול, אלו בדיוק המקרים שבהם החברים החדשים שלנו

מצילים אותנו באמצעות האינטליגנציה המלאכותית שלהם. מעבר לשיקולי האבטחה המובנים מאליהם אותם עוזרים אישיים מאזינים לנו כל היממה בסוף היום - צצה בראשו מחשבה נוספת: האם ייתכן שאנחנו מתעלמים מהאיום של אנשים זדוניים שינסו לנצל את המכשירים האלה כדי לפלוש לחיינו הפרטיים? תוך כדי כך, לא יכולנו שלא לשאול שאלה נוספת: האם אנחנו בכלל מודעים לכמות וסוג המידע שאנחנו משתפים עם הגאדג'טים האלה?

הונאות ממשיכות להתחזות למיילים שנשלחים כביכול מהבנק

עברייני הרשת ממשיכים להונות אותנו באמצעות מיילים בהולים שנשלחים כביכול מטעם הבנקים ומשדלים קורבנות תמימים למתן פרטי כניסה לחשבונות בנקים ופרטי כרטיסי אשראי.

גם לאחרונה הופץ מייל המתחזה לבנק לאומי ודורש אימות פרטי חשבון לפני סגירתו. בחודש שעבר היה זה מייל מטעם בנק ירושלים השיטה זהה הנראות שונה. המטרה של שולחי המיילים האלו היא לדלות פרטים רגישים כמו פרטי כניסה לחשבונות בנק, פרטי כרטיס אשראי על מנת לנצל אותם לרעה.

המייל המתחזה לבנק לאומי נושא את הכותרת "עדכן את החשבון שלך עכשיו" ונשלח בשם Leumi Bank מהכתובת fha@servicemail.net בלחיצה על הקישור הלקוח מופנה לאתר של בנק לאומי והקורבן מתבקש להזין פרטי כניסה לחשבון, לאחר מכן פרטים אישיים כמו דוא"ל, ת.ז וסיסמאות ולבסוף מתבקש להזין פרטי כרטיס אשראי. בסוף התהליך על מנת לשוות לו אמינות הלקוח מופנה מחדש לאתר האמיתי של בנק לאומי. במקרה של הפישינג המתחזה לבנק לאומי מגדילים התוקפים ומנסים לגנוב גם את פרטי הגישה לאימייל וגם את פרטי כרטיס האשראי. כך במקרה שהקורבן ינסה לאפס סיסמה לגישה לחשבון שלו, וישלח מייל איפוס לחשבון המייל שלו, התוקפים יירטו את המייל וימנעו מהקורבן לחסום את הגישה שלהם לחשבון.