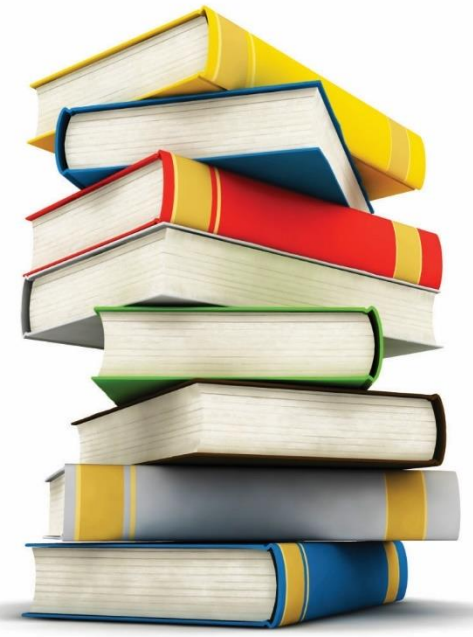


תוכן עניינים

כל אחד יכול ליצור אלגוריתם שהוא עצמו לא יכול לשבור. זה אפילו לא קשה. מה שקשה הוא ליצור אלגוריתם שאף אחד אחר לא יכול לשבור, גם אחרי שנים של עבודה.
ברוס שנייר

2022 | דצמבר | 1

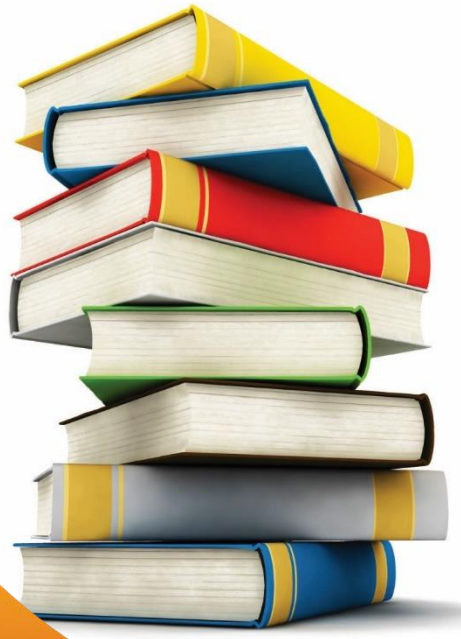
1. קבוצת רמאים מתוחכמת גנבה לפחות 480 מיליון אירו מקורבנות בצרפת, בלגיה ולוקסמבורג מאז 2018. לפי חוקרים ב-Group-IB. החבורה משתמשת בערכת הונאה מתוחכמת ביותר בשם "CryptosLabs", המתחזה לפורטלי השקעות של יותר מארבעים גופים פיננסיים גדולים באירופה.

מערכת ההונאה מבטיחה לקורבנות תשואות גבוהות על הונם. כדי למצוא את ה'משקיעים', הרמאים משאירים הודעות בפורומי ההשקעות או משתמשים במנגנוני פרסום לגיטימיים במדיה החברתית ובמנועי החיפוש כדי לקדם את תכנית המרמה. כדי להציג אמינות, מודעות כאלה מציגות לוגו של חברות בולטות מתחומי בנקאות, פין-טק, קריפטו וניהול נכסים הפעילות בצרפת, בלגיה ולוקסמבורג.

לקריאת המאמר המלא

מה למדנו? אם זה טוב מכדי להיות אמיתי, כנראה שזה לא אמיתי. בצעו את בדיקות הנאותות שלכם ביסודיות ובזהירות.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them



2. כישורי סייבר מממנים מאמצים צבאיים

שירותי המודיעין של דרום קוריאה, המשטרה הלאומית וחמישה משרדים ממשלתיים פרסמו אזהרה על הטקטיקות של צפון קוריאה (DPRK) שפועלות כך:

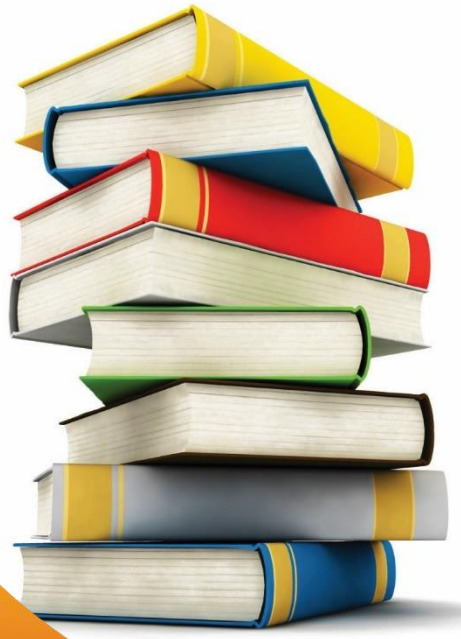
עובדי מחשבים של DPRK ממוקמים בכל רחבי העולם, ומערפלים את הלאום והזהות שלהם. הם מרוויחים מאות מיליוני דולרים בשנה על ידי עיסוק במגוון רחב של עבודות פיתוח IT, כולל פיתוח ותחזוקה של פלטפורמות עבודה עצמאיות (אתרים/אפליקציות) ופיתוח מערכות מטבעות קריפטוגרפיים.

תפקידם האמיתי של אותם עובדים, נטען באזהרה, הוא "להרוויח מטבע חוץ ולממן תוכניות גרעין וטילים עבור המשטר".

לקריאת המאמר המלא

מה למדנו? בדקו היטב את מי אתם מעסיקים ולמי משלמים. אולי אתם עוזרים לרעים לממן את המאמצים הצבאיים שלהם.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them



3. ההיסטוריה של פישינג מ-1996 עד 2022

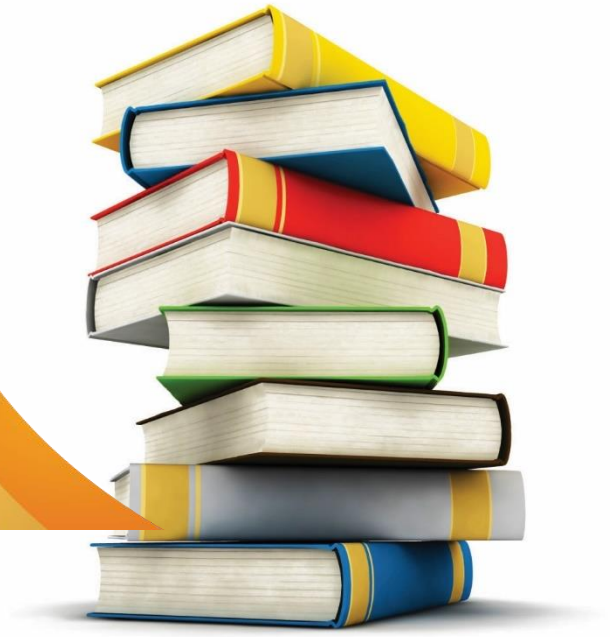
2022 | דצמבר | 1

המונח "דיוג" נטבע עוד בשנת 1996, כאשר פושעי סייבר תקפו משתמשים של America Online (AOL), ספקית האינטרנט הגדולה ביותר באותה תקופה. בעודם מתחזים לעובדי AOL, הרמאים שלחו הודעות וביקשו מהמשתמשים לאמת את החשבונות שלהם או ביקשו פרטי תשלום. שיטה זו של פישינג לגניבת נתונים אישיים עדיין בשימוש היום, מכיוון שלמרבה הצער, היא ממשיכה להניב תוצאות.
בשנות ה-90 הופיעו ההונאות המקוונות הראשונות. כשהבנקים החלו להפעיל בנקאות באינטרנט, רמאים שלחו הודעות טקסט למשתמשים, כביכול מקרובי משפחה, עם בקשה דחופה להעביר כסף לפי פרטים שנמסרו בהודעה.
בתחילת שנות ה-2000, צדקה הפכה למישור הונאה נפוץ: למשל, לאחר רעידות אדמה והצונאמי של האוקיינוס ההודי של 2004, משתמשים קיבלו הודעות מארגוני צדקה מזויפים שהתחננו לתרומות. בערך באותו זמן, התוקפים החלו להתמקד במערכות תשלום מקוונות ובבנקאות אינטרנט. מכיוון שחשבונות משתמש באותם ימים היו מוגנים רק על ידי סיסמה☹, זה הספיק לתוקפים לגנוב את הסיסמא כדי לקבל גישה לכספם של הקורבנות. לשם כך הם שלחו מיילים בשם חברות כמו PayPal, וביקשו מהמשתמשים להיכנס לאתר מזויף המציג את הלוגו של החברה ולהזין את הסיסמא שלהם. כדי לגרום לאתרים שלהם להיראות אמינים יותר, פושעי סייבר רשמו מספר דומיינים, כולם דומים מאוד למקור, ונבדלים זה מזה רק בשתיים או שלוש אותיות. משתמש לא קשוב יכול בקלות ובטעות לא להבדיל בזיוף שהוא אתר בנק או מערכת תשלומים אמיתית. בנוסף, הרמאים השתמשו לעתים קרובות במידע אישי מרשתות חברתיות של הקורבנות עצמם כדי להפוך את ההתקפות שלהם לממוקדות יותר, ובכך להצליח יותר.
ככל שהזמן התקדם, הונאות מקוונות נעשו מתוחכמות ומשכנעות יותר ויותר. פושעי סייבר למדו כיצד לחקות בהצלחה את האתרים הרשמיים של מותגים, ולהפוך אותם לכמעט בלתי ניתנים להבחנה מהמקור ולמצוא דרכים חדשות לפנות לקורבנות. בהמשך הופיעו שירותים המתמחים ביצירת תוכן מזויף, ובשלב זה הדיוג באמת המריא. כעת לא רק הנתונים האישיים והכספים של משתמשים רגילים היו בקו האש, אלא גם פוליטיקאים ועסקים גדולים.
דוח זה בוחן את המגמות, השיטות והטכניקות העיקריות של פישינג שפועלות בשנת 2022.

לקריאת **המאמר המלא**

מה למדנו? המאמר המלא מעניין מאוד, כולל דוגמאות בשפות שונות ויעזור לכם לחזק את המודעות שלכם.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

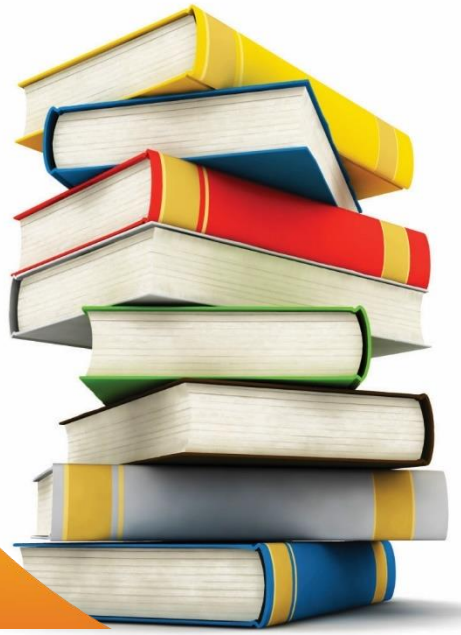


4. מי פגיע יותר להתחזות?
צעירים או מבוגרים?
נשים או גברים?

על פי נתונים חדשים מחברת ההדרכה למודעות אבטחה SoSafe,
הדור הדיגיטלי בגילאי 18-39 הם קבוצת הגיל הפגיעה ביותר להונאות דיוג.
הדוח מגלה שלבני 18-39 יש שיעור הקלקה ממוצע של 29 אחוז על הודעות דיוג, אשר יורד ל-19 אחוז בקרב קבוצות גיל מבוגרות יותר.
הדוח גם מראה שגברים נוטים ללחוץ על קישורי דיוג לעתים קרובות יותר מנשים.
23 אחוז מהגברים פתחו לפחות אחד ממייל הדיוג המדומה, כאשר שיעור ההקלקה הממוצע בקרב המשתתפות נמוך ביותר מ-10 אחוזים.
ארגונים במגזר הציבורי הם הפגיעים ביותר להתקפות פישינג (עם שיעור הקלקה ממוצע של 36 אחוזים), בעוד שעובדים בחברות ייצור נוטים פחות ללחוץ על מיילים מזיקים (19 אחוז).

לקריאת המאמר המלא
מה למדנו? כולנו פגיעים. חלק יותר וחלק אפילו יותר.
גבר צעיר במגזר הציבורי הוא הפגיע ביותר. 😊

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them



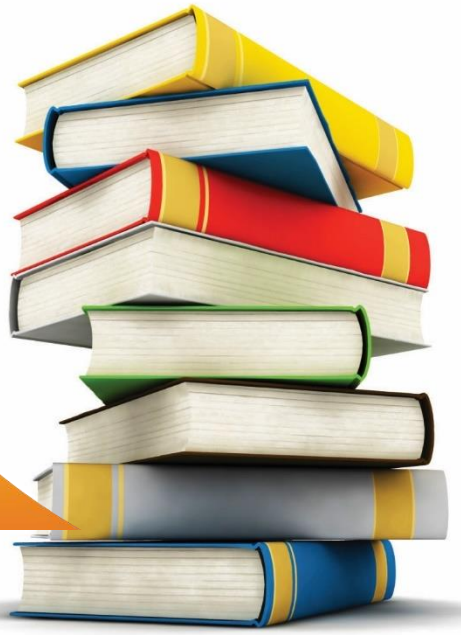
5. היזהרו אם אתם מטרידים אנשים, ייתכן שזו חרב פיפיות

אנשים רבים סבלו ממקרים מפחידים של הטרדה. זה עשוי היה לכלול הודעות טקסט רבות ומאיימות, אינספור מיילים ומשלוחי חבילות פיזיותם. מובן שזה הפריע להם לא לדעת את זהות המטריד שלהם. במקרה הזה הם יודעו, והנה פרטים על החקירה. אתר בשם "Get Revenge On Your Ex" (https://www.getrevengeonyourex.com) קיים כבר למעלה מעשור. זהו אחד מני שירותים רבים אשר יפציצו בהודעות טקסט ואימיילים את הקורבן תמורת תשלום קטן. בספטמבר 2022, האתר נפרץ וכל נתוני המשתמשים נגנבו. בעוד שרוב פריצות חושפות פרטים מזיקים שעלולים לפגוע בקורבנות חפים מפשע. במקרה זה אנו נתקלים בתקיפה שחשפה את הפושעים (המטרידים) שחשבו שהם אנונימיים. אני מאמין שזה סוג ההצלחה שצריך לדון בו בדיונים על האתיקה של גישה לנתונים.

לקריאת המאמר המלא.

מה למדנו? מי שמשתמש ב-PayPal או אפילו ב-crypto כדי לשלם עבור שירותים מפוקפקים, חשופים מאוד. ברגע שהחקירה המקוונת מתחילה לחפור בנתונים אלה, החשיפה הופכת לכואבת ולא נעימה.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them



6. שאלה מהגיליון הקודם:

2022 | דצמבר | 1

מהי ההגנה הטובה ביותר נגד תוכנות כופר?
א. רכישת ביטוח סייבר מקיף.
ב. גיבוי הנתונים באופן קבוע.
ג. עדכון באופן קבוע של כל המכשירים והתוכנות עם תיקוני האבטחה העדכניים ביותר.
ד. השתמשו בכלי אנטי וירוס טוב.

התשובה הנכונה היא "ב"
א – אולי יחזיר לכם כסף אך לא את הנתונים
"ג" ו "ד" חשובים אך לא יכולים להבטיח הגנה של 100%

שאלה חדשה
אתם מקבלים הודעת טקסט מספק שמבקש מכם ללחוץ על קישור לחידוש הסיסמה כדי שתוכלו להיכנס לאתר שלו. עליכם: (נא לסמן את כל התשובות הנכונות)
א. השיבו להודעת הטקסט כדי לוודא שאתם באמת צריכים לחדש את הסיסמה.
ב. הרימו טלפון והתקשרו לספק, באמצעות מספר טלפון שאתם יודעים שהוא נכון, כדי לוודא שהבקשה אמיתית.
ג. לחצו על הקישור. אם זה לוקח אתכם לאתר של הספק, אז תדעו שזו לא הונאה.
ד. היכנסו לאתר הספק באמצעות קישור שאתם יודעים שהוא נכון ובדקו שם אם צריך לחדש סיסמא