אאוץ! | פברואר 2019

SANS SECURITY AWARENESS

OUCH!

עלון מודעות אבטחת מידע למשתמשי מחשב

הונאה מותאמת אישית

סקירה כללית

פושעי סייבר ממשיכים להמציא דרכים חדשות ויצירתיות לשטות באנשים. סוג חדש של הונאה הצובר פופולריות הוא הונאה מותאמת אישית. פושעי סייבר מוצאים או רוכשים מידע על מיליוני אנשים, ולאחר מכן משתמשים במידע זה כדי להתאים אישית את ההתקפות שלהם. אנו נראה לך כיצד הונאות אלה עובדות ונלווה אותך באמצעות דוגמאות. ככל שאתה יודע יותר על הונאות אלה, יותר קל לך לזהות ולעצור אותם.

איך זה עובד?

הונאות דואר אלקטרוני או שיחות טלפון אינם חדשים, פושעי סייבר מנסים לשטות אנשים כבר שנים. הדוגמאות כוללות את: "זכית בהגרלה" או ההונאה הידועה לשימצה "הנסיך הניגרי". עם זאת, אלה הונאות מסורתיות, ופושעי הסייבר לא יודעים על מי הם מתמקדים. הם פשוט יוצרים מסר כללי ושולחים אותו למיליוני אנשים. בגלל שהונאות אלה כל כך גנריות, בדרך כלל קל לזהות אותן. הונאה מותאמת אישית שונה, פושעי הסייבר חוקרים ,תחילה כדי ליצור הודעה מותאמת אישית עבור כל קורבן מיועד. הם עושים זאת על ידי מציאת או רכישת מסד נתונים של שמות אנשים, סיסמאות, מספרי טלפון או פרטים אחרים. סוג זה של מידע זמין בקלות בשל כל האתרים אשר נפרצו. המידע גם זמין בדרך כלל באתרי מדיה חברתית ורשומות ממשלה הזמינים לציבור. לאחר מכן הפושעים מתמקדים על כל מי שיש להם מידע עליו.

אחד הטריקים הנפוצים שפושעי סייבר משתמשים בו הוא הפחדה או סחיטה כדי לאלץ אותך לשלם להם כסף. ההתקפה עובדת כך, הם מוצאים או רוכשים מידע של שמות משתמשים וסיסמאות מאתרים שנפרצו. הם מוצאים את פרטי החשבון שלך הכלולים במסד נתונים כזה ושולחים לך (ולכל השאר במסד הנתונים) דוא"ל עם פרטים אישיים אודותיך, כולל הסיסמה המקורית שבה השתמשת לאתר שנפרץ. הפושע מתייחס לסיסמה שלך כמו "הוכחה" של פריצה למחשב שלך או לכל מכשיר אחר, וזה כמובן לא נכון. הפושע גם טוען כי בזמן שהם פרצו למחשב הם גם תפסו אותך צופה פורנוגרפיה באינטרנט. הדוא"ל שנשלח אלייך מאיים שאם לא תשלם את דמי הסחיטה שלהם, הם ישתפו עם המשפחה שלך וחברים ראיות של פעילויות מביכות באינטרנט.

המלכוד הוא, שבכמעט בכל מצב כזה פושע הסייבר מעולם לא פרץ את המערכת שלך. הם אפילו לא יודעים מי אתה או באילו אתרים ביקרת. הנוכל פשוט מנסה להשתמש בפרטים האישיים שלך שברשותו על מנת להפחיד אותך ולגרום לך להאמין שהם פרצו את למחשב או למכשיר שלך, כדי להונות אותך לשלם להם כסף. זכור, הרעים יכולים להשתמש באותה טכניקות גם עבור הונאת טלפון.

מה עלי לעשות?

זהה כי הודעות דוא"ל או שיחות טלפון כאלה הן תרמית. זה טבעי להרגיש פחד כאשר למישהו יש מידע אישי עלייך. עם זאת, זכור שהשולח משקר. ההתקפה היא חלק ממסע פרסום אוטומטי בקנה מידה המוני, לא ניסיון להתכוון עליך ישירות. היום לפושעי סייבר הרבה יותר קל למצוא או לרכוש מידע אישי, אז צפה ליותר הונאות אישיות כמו אלה בעתיד. להלן מספר רמזים לחפש תרמית זו:

- **בכל פעם שאתה מקבל הודעת דוא"ל דחופה, הודעה או שיחת טלפון חשודים מאוד. אם מישהו משתמש ברגשות כמו פחד או דחיפות, הם מנסים לזרז אותך לעשות טעות.**
- **כאשר מישהו דורש תשלום ב BitCoin, כרטיסי מתנה, או שיטות אחרות שלא ניתן לעקוב אחריו.**
- **כאשר אתה מקבל דוא"ל חשוד, חפש ב- Google כדי לראות אם אנשים אחרים דיווחו על התקפות דומות כאלה.**

בסופו של דבר השכל הישר הוא ההגנה הטובה ביותר שלך. עם זאת, אנו ממליצים שתשתמש תמיד בסיסמה ארוכה וייחודית עבור כל אחד מהחשבונות המקוונים שלך. לא זוכר את כל הסיסמאות שלך? השתמש במנהל סיסמאות. בנוסף, אפשר אימות דו-שלבי ככל שניתן.

עורך אורח

לני לנצ'ר מנוסה באבטחת מידע. בונה פתרונות נגד תוכנות זדוניות במעבדות Minerva ומלמד כיתות אבטחה במכון SANS. ניסיונו כולל גם שירותי אבטחה מנוהלים וייעוץ. עקוב אחריו ב- zeltser.com/blog *מתמחה בOSINT. הוא אוכל, ישן, ונושם כל מה שקשור לאיסוף* @lennyzeltser.

מקורות

הנדסה חברתית: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_he.pdf
לעצור את הדייג: https://www.sans.org/sites/default/files/2018-04/201804-OUCH-April-Hebrew.pdf
חפש את עצמך באופן מקוון: https://www.sans.org/sites/default/files/2019-01/201901-OUCH-January-Hebrew.pdf
מנהל הסיסמאות: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201709_he.pdf