



דו"ח הגנת דיגיטלית של בן סמית

תדירות הדו"ח: שבועית

אנליסט: ירון בכור

תאריך: 3 במאי, 2024

VIP : בן סמית, מנכ"ל חברת Tren Industries

תמצית מנהלים

הדו"ח השבועי מזהה איומים משמעותיים לבטיחותו וביטחונו הדיגיטלי של מר בן סמית. איומים כגון, אלימות, תכנון להפגנה בקרבת מגוריו, דליפת מידע אישי מזוהה (כולל מידע בסיכון פוטנציאלי גבוה), ופרטי גישה למדיה חברתית שהודלפו, תורמים כולם לסביבת סיכון מוגברת. רמת הסיכון הכללית של מר בן סמית מוערכת כגבוהה.

פעילות הניטור

א. ניטור רשת האפלה

כלים ספציפיים בשימוש: DarkOwl, Lunar Webz

כיסוי הניטור: מדיה חברתית AltTech, (מדיות חברתיות בלתי מצונזרות כגון Gab, Bitchite ועוד 30 נוספים) פורומים, שווקים, אתרי הדבקה, אתרי בצל ספציפיים, טלגרם, דיסקורד.

ב. ניטור מאגרי נתונים שהודלפו

מקורות בשימוש: BreachDirectory, haveibeenpwned.com, שירות הודעות על הפרות ספציפיות Lunar Webz ,

ממצאים

א. איום באלימות

איום קיצוני לרצוח את מר סמית זוהה בפורום של דברי שנהא ב-12 במרץ, 2024 (צילום מסך 1 - הוסר).

האיום הגיע ממשתמש בשם "Fire_starter99" (שם המשתמש הוסר) ומתייחס לתפקידו של מר סמית ב. Tren Industries. פרטים לגבי התוכנית הפוטנציאלית נמצאים כעת בחקירה. (הערה: בשל האופי הרגיש של ממצא זה, נכללו כאן פרטים מוגבלים. חקירה נוספת ואמצעי אבטחה פוטנציאליים יטופלו בנפרד).

ב. הפגנה מתוכננת

מידע על הפגנה מתוכננת בקרבת ביתו של מר סמית במאליבו, קליפורניה התגלה בדף אירוע ברשת החברתית (צילום מסך 2 - הוסר) ב-20 באפריל, 2024.

האירוע, שותרתו "הפגנה נגד נוהלי הסביבה של Tren Industries" מתוכנן ל-18 במאי, 2024, בשעה 14:00 לפי שעון מערב ארה"ב. פרטים לגבי המארגנים והגודל הפוטנציאלי נבדקים לצורך הערכת סיכוני האבטחה האפשריים.

ג. חשיפת מידע אישי (PII)

פוסט מ doxbin.org מ-1 באפריל, 2024 (צילום מסך 3) חשף את המידע האישי של מר סמית, כולל כתובת מגוריו (1234 Pacific Coast Highway, Malibu, CA 90265) ומספר הטלפון שלו (הוסר לצורך הדו"ח).

אימות אישר את הלגיטימיות של הפוסט, מה שמעיד על חשיפה בסיכון גבוה. מידע אישי ספציפי שהודלף (הוסר לצורך הדו"ח) מהווה סיכון משמעותי לגניבת זהות או התקפות ממוקדות.

ד. חשבון מדיה חברתית שנפרץ

פוסט בפורום ההאקרים הרוסי nulled.to מ-27 באפריל, 2024 (צילום מסך 4 - הוסר) חשף פרטי גישה שנפרצו לחשבון האינסטגרם האישי של מר סמית (@bensmith_private).

הפוסט מציין שהחשבון נפרץ ושפרטי הכניסה (שם משתמש וסיסמה - הוסרו לצורך הדו"ח) נמכרים תמורת 200 דולר אמריקאי במטבע קריפטו.

הדבר מהווה סיכון להשתלטות על החשבון, נזק תדמיתי, והתקפות הנדסה חברתית פוטנציאליות תוך ניצול המידע הגנוב.

הערכת הסיכונים

בהתבסס על הממצאים שזוהו, רמת הסיכון הכללית לביטחוננו הדיגיטלי של מר בן סמית מוערכת כגבוהה.

השילוב של איום אמין באלימות, הפגנה מתוכננת, דליפת מידע אישי, ופרטי גישה שנפרצו לחשבון מדיה חברתית יוצר סביבה סיכונית מורכבת ומדאיגה.

המלצות

פעולות מיידידות

תיאום עם אנשי האבטחה הרלוונטיים להערכת וטיפול באיום האלימות.

הגברת אמצעי האבטחה הפיזיים סביב ביתו של מר סמית במאליבו, קליפורניה, לקראת ההפגנה המתוכננת ב-18 במאי, 2024.

יצירת קשר עם doxbin.org לבקשת הסרת המידע האישי של מר סמית.

אבטחת חשבון האינסטגרם שנפרץ (@bensmith_private) באמצעות איפוס סיסמה והפעלת אימות דו-שלבי (MFA).

ניטור מתמשך

המשך ניטור הרשת האפלה ומאגרי הנתונים שהודלפו לאיתור איומים או חשיפות נוספות.

שיפור ניטור המדיה החברתית לאיתור ניסיונות התחזות או פריצות נוספות.

הדרכת מודעות אבטחה

יש לשקול לספק למר סמית הדרכת מודעות אבטחה לזיהוי והפחתת התקפות הנדסה חברתית.

שיקולים נוספים: אבטחת מכשיר נייד

במקרה של חשד להדבקה תוכנה זדונית במכשיר הנייד של מר סמית, להלן ההמלצות.

בידוד המכשיר: אם אפשר, יש לבודד מיד את מכשיר הנייד של מר סמית מכל חיבורי רשת Wi-Fi נתוני סלולר (כדי למנוע המשך גניבת נתונים או תקשורת פיקוד ובקרה אפשרית מצד התוכנה הזדונית).

סריקת אבטחה: יש להשתמש באפליקציית אבטחה ניידת אמינה כדי לבצע סריקה יסודית של המכשיר לאיתור תוכנות זדוניות. אפשרויות פופולריות ניתן למצוא ברשת.

סקירה ידנית: אם אין אפליקציית אבטחה אמינה זמינה, יש לשקול סקירה ידנית של האפליקציות שהותקנו לאחרונה, עם דגש על אלה שהורדו ממקורות לא מהימנים. אפליקציות לא מוכרות או חשודות יש להסיר.

גיבוי נתונים (אופציונלי): אם התוכנה הזדונית אינה קריטית ונראית יחסית תחת שליטה, שקול לגבות נתונים חיוניים מהמכשיר (אנשי קשר, תמונות) רק אם אתה בטוח שתהליך הגיבוי לא יסכן את הנתונים הלא נגועים.

סיוע מומחה אבטחה: במקרה של זיהומי תוכנה זדונית מורכבים או אם ההמלצות לעיל נחשבות למסוכנות מדי, מומלץ מאוד להתייעץ עם מומחה לאבטחת מכשירים ניידים. הם יכולים לספק ניתוח מעמיק יותר ולבצע תהליך הסרה בטוח.

נספח

ניתן להשתמש בסעיף זה לאחסון אינדיקטורים טכניים מפורטים (IOCs) הקשורים לאיומים שזוהו, יומני תקשורת או צילומי מסך מלאים ולא מצונזרים לצורך עיון פנימי. זכור לאחסן מידע זה בצורה מאובטחת.

הערה, דו"ח זה מדגיש חששות אבטחה קריטיים הדורשים תשומת לב מיידית. חקירה נוספת ואמצעי אבטחה פוטנציאליים יטופלו בתקשורת נפרדת.

לתשומת לבך, כל שמות המשתמש, הכתובות ומידע מזהה אחר הוסרו מהדו"ח הזה צילומי המסך (1-4) הם תחליפים.

חשיפת המידע האישי (PII)

```
[96436, 'Omnipotentupgrade', 144, 'Omnipotent upgrade', 'opsec  
\\nhttps://raidforums.com  
\\nraidforums owner full name :  
\\naddress  
1: (Postal Code) CPN (Door No: ) (http://puu.sh/ ) ( Aprox )  
2: (Street) 123 Cr  
ra@raidforums.com  
a@pro@protonmail.com  
le@suggestions4techfirst@gmail.com  
ro@predator.wtf  
pa@raidforums.com  
di@liver@hotmail.com  
je@live.com.pt  
di@ly25@gmail.com  
o@ment@raidforums.com  
de@loadedfrom@raidforums.com  
de@loadedfrom@raidforums.com  
he@live.co.uk  
ol@jok@hotmail.com  
di@live.com.pt  
\\nPaypal Accounts  
\\nroot@predator.f-  
Name On Account : Kevin  
Number On Account : 07*** **9743[U+202C]  
Paypal Account Address : N/A  
\\nleavesug@techfirst@gmail.com -  
Name On Account : Omnipotent  
Number On Account : +44.77492 (07xxx-xxxxxx)  
Paypal Account Address : 123 Cr on Rd Door  
880 x 520
```

ההפגנה מול ביתו של בן

