קומסקיור בע"מ

23/05/10

- הודעה לעיתונות -

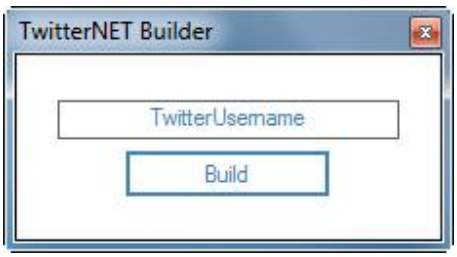
ציוץ קטלני - חברת ESET מתריעה בפני נוזקה המופצת ברשת החברתית - טוויטר

רנדי אברמס, מנהל המחלקה למודיעין על נוזקות במרכז הפיתוח האמריקאי של חברת האנטי וירוס ESET, וחוקר נוזקות בכיר, כתב לפני מספר ימים בבלוג שלו על כלי חדש שמופץ כיום ברשת האינטרנט שנועד ליצירת סוסים טרויאנים שעושים שימוש ברשת החברתית טוויטר.

הפצת נוזקות באמצעות המדיה החברתית הוא אחד הטרנדים החזקים ביותר בתחום הנוזקות היום. פיתוח של נוזקות וכלים שעושים שימוש ברשתות חברתיות על מנת להפיץ את עצמם לכמות גבוהה ככל הניתן של מחשבים ורשתות. הקלות היחסית בה ניתן לגנוב זהויות או לשלוח הודעות ולהעלות פוסטים שמכילים קישורים לאתרים מהם מושתל קוד זדוני במחשב הקורבן המיועד מעודדת את כותבי הנוזקות להמשיך ולחפש דרכים יצירתיות לשימוש ברשתות החברתיות.

התפיסה הרווחת היא שישנם האקרים "יחידי סגולה" בעולם שמשתמשים בתכנות של קוד מתוחכם על מנת ליצור נוזקות חדשות ולמצוא פרצות אבטחה במערכות הפעלה או אתרים פופולאריים. האמת העצובה היא שהימים הללו חלפו כבר לפני יותר מעשור, וכיום מיוצרים כלים בצורה מאורגנת, לרוב במימון משפחות פשע, שנותנים לכל בעל ידע בסיסי ביותר בשימוש במחשב ליצור נוזקות חדשות במספר קליקים, או להשתמש בכלים שמאפשרים התקפות על רשתות עם אבטחה גבוהה מהממוצע.

הכלי שעליו כתב רנדי אברמס שנקרא TwitterNet Builder, הוא עוד דוגמא לכלי שמאפשר יצירה של וריאנטים (variants) שהם בעצם סוג של מוטציות של נוזקות קיימות, שאינן מזוהות ע"י חלק מתוכנות האבטחה הנפוצות כיום משום שהן מכילות קוד ששונה במעט מהנוזקה המקורית. הכלי שמזוהה ע"י ESET NOD32 Antivirus בתור MSIL/Agent.NBW הוא כלי פשוט ביותר שהממשק שלו נראה כך:



כל מה שהתוקף צריך לעשות, הוא ליצור פרופיל חדש בטוויטר, ממנו הוא יבצע את ההתקפות על הקורבנות המיועדים שלו. לאחר שמוקלד שם הפרופיל בשדה העליון במקום הטקסט TwitterUsername, בלחיצה על הכפתור Build ייווצר קובץ הפעלה עם סיומת EXE שהוא בעצם וריאנט חדש של סוס טרויאני. לאחר שהתוקף משנה את שם הקובץ לשם מפתה כלשהו (לדוגמא: קטע מצונזר מהאח הגדול.exe), ניתן לשתול את הסוס הטרויאני במחשבים של קורבנות במגוון שיטות פשוטות יחסית, שפירטתי

בית אל-על קומה 10, בן יהודה 32 תל אביב מען לדואר: ת.ד. 11032 ת"א 61116	טלפון: 03-6290845 פקס: 03-6208178	Info@eset.co.il www.eset.co.il

PDF created with FinePrint pdfFactory Pro trial version www.pdffactory.com

את חלקן בכתבה האחרונה שלי. המשמעות היא שגם אימא שלי יכולה היום, אם היא רוצה, להפוך להאקרית ממולחת שגונבת מידע וסיסמאות ממאות ואלפי קורבנות תמימים (בלי לזלזל ביכולת הגבוהה של אמא שלי בשימוש במחשבים וטכנולוגיה).

ברגע שהקורבן המיועד מתפתה להפעיל את הקובץ שמכיל את הסוס הטרויאני, הוא יישאר פעיל ברקע במערכת ההפעלה עד לרגע שבו תתקבל פקודה שתישלח מהתוקף. את הפקודה הוא שולח באמצעות "ציוץ" שמפורסם בפרופיל של הקורבן בתור תגובה או בתור פוסט חדש. דוגמא לפקודות בסיסיות שניתן לשלוח לסוס הטרויאני:

- הפקודה DDOS * IP * PORT מפעילה "התקפת מניעת שירות" שהיא התקפה שמשמשת להשבתת חיבור האינטרנט או מערכת ההפעלה של הקורבן המיועד.
- הפקודה DOWNLOAD * LINK / MALWARE.EXE היא פקודה שמורידה למחשב הקורבן נוזקה או נוזקות נוספות, שמאפשרות לתוקף שליטה גדולה יותר במחשב הקורבן, ואפשרויות תקיפה נוספות.
- הפקודה REMOVEALL מסירה את הסוס הטרויאני ממחשב הקורבן, וכל זכר נוסף שעלול לרמז שנגנב מידע או שבוצעה פעולה לא רצויה באותה המערכת.

רנדי אברמס מגיע בקרוב לביקור בארץ, וירצה במסגרתו על טרנדים חדשים בנוזקות ואבטחת מידע.

אודות ESET

חברת ESET הינה ספקית בינלאומית של תוכנת האבטחה NOD32 וחבילת האבטחה ESET Smart Security לארגונים בגדלים שונים וצרכנים פרטיים. החברה מתמחה בפיתוחי טכנולוגיות מתקדמות של אבטחת מידע ומתמקדת בפיתוחים מורכבים, מאופיינים ביעילות חסרת תקדים אשר מותירים עקבות מזעריים במערכת. החברה מיוצגת ברחבי העולם כולו ביותר מ-100 מדינות וסניפיה המרכזיים ממוקמים היום באנגליה, ארגנטינה, סלובקיה וכמובן ארצות הברית. בישראל, מיוצגת ESET באופן בלעדי על ידי חברת קומסקיור, המפעילה בארץ מרכז פתרונות ותמיכה טכניים בשפה העברית.

בית אל-על קומה 10, בן יהודה 32 תל אביב מען לדואר: ת.ד. 11032 ת"א 61116	טלפון: 03-6290845 פקס: 03-6208178	Info@eset.co.il www.eset.co.il

PDF created with FinePrint pdfFactory Pro trial version www.pdffactory.com