דמי חסות וחטיפות ברשת

ד"ר דוד פסיג בפינת רדיו עם רון נשיאל בתוכניתו השבועית "מעבירים לראשון" 2 ביולי 2005

כולם עסוקים בסוסים טרויאנים אבל מה דעתך, רון, שיש משהו הרבה יותר מפחיד בדרך, שכדאי לא רק לבתי עסק גדולים להזהר ממנו אלא גם אנחנו האנשים הפרטיים שמחוברים לרשת צריכים לפקוח את עיננו בו.

אני רוצה להקדיש את הפינה שלנו הפעם לסוג חדש של פשיעה ברשת שהתגלתה לאחרונה וסביר להניח כי היא תלך ותגבר בעתיד.

ממש לאחרונה, ה-FBI הוציאו אזהרה מוזרה בה הם טוענים כי גילו מספר מקרים בהם פושעים, מומחי מחשבים, הצליחו לפתח וירוס מסוג חדש לחלוטין אשר מצליח להצפין מסמכים במחשבים שנדבקו בו עד אשר בעל המחשב משלם כופר בסכום נקוב ורק אז נותנים לו את הקוד כיצד לפתוח את המסמכים שהוצפנו.

ב-FBI טוענים כי למזלם של אלו שנדבקו בוירוס החדש שיטת ההצפנה שהפושעים השתמשו בה לא היתה קשה במיוחד לפיצוח. הפחד שלהם הוא ששיטת ההצפנה בפעם הבאה תהיה מורכבת במיוחד ואז הפושעים הללו יוכלו לבקש סכומים גדולים מאנשים שידבקו בוירוס.

הוירוס עובד כך: הוא מחפש במחשב של הקורבן מסמכים מחמשה עשר סוגים שונים- וורד, אקסל, ועוד, ומצפין אותם. אחר כך הוא מעלה חלונית בה בעל המחשב מתבקש לשלם סכום של 200$ כופר אם הוא רוצה לקבל את התוכנה שתפצח את ההצפנה של המסמכים שלו.

הוירוס הזה בעצם מנצל טכנולוגיה שאמורה להגן על הנתונים שלנו ולא לחטוף אותם. מה שמעליב הוא שהוירוס הזה שומר את המסמכים החטופים מול עיניו של בעל המסמכים.

הוירוס התגלה רק לפני כשבועיים שלושה. והוירוס מדביק את המחשב דרך שיוט באתרים שונים ולא דרך הדואר האלקטרוני. הוא מנצל פרצת אבטחה בדפדפן ומוריד למחשב מסמך בשם PGPCODER וזה מתחיל לעשות את עבודתו. השם של המסמך יכול להטעות את המבינים שביננו כי הוא משתמש בראשי התיבות של תוכנות קוד פתוח שאמורות לשמור על ההצפנה שלנו. PGP הם ראשי התיבות של Pretty Good Privacy.

אגב זו לא הפעם הראשונה שאנחנו רואים גירסאות של קונצפט פשיעה כזה. היו נסיונות לשתול תוכנות כאלו באתרים של קזינו למינהם בהם הודיעו לבעלי הקזינו שאם לא

פושעי רשת הופכים להיות מתוחכמים בדרכים שלא יאומנו. והם רק התחילו לגלות את הרשת כדרך נהדרת לעשות קופה. במקרה אחר שגם התפרסם לאחרונה. התגלה וירוס בשם Myfip שתפקידו היה לחטוף תוכניות עיצוב של מוצר חדש של חברה מסויימת. כשזה הצליח הוא העלה הודעה בה היתה כתובה הדרישה שאם לא ישולם כופר בסך כך וכך הוירוס ישלח את התוכניות לחברה סינית שתייצר העתקים זולים של אותו המוצר.

הדרך לטפל בסוג חדש זה של וירוסים כמוכל שאר הוירוסים היא פשוטה למי שעיניו בראשו. קודם כל להשתמש בתוכנות אנטי וירוס מעודכנות. ב. להוריד את עידכוני האבטחה האחרונים למערכת ההפעלה שלך ולדפדפנים שברשותך. אבל הכי חשוב...זו המלצה שלי אחר שנשרפתי לאחרונה. לערוך גיבויים כל יום לעבודה שלך...לא רק פעם בכמה זמן... ולא גיבוי אחד...אלא לפחות שלושה עד חמשה.

היום זה ממש קל... הדיסקים החיצוניים זולים מאוד והם בעלי נפחים גדולים. וגם, הם מגיעים עם תוכנות פשוטות. יש אפילו גרסאות של דיסקים חיצוניים שיש עליהם כפתור אחד ובלחיצה על הכפתור אתה מגבה את כל הדיסק הקשיח שלך...וזה כמובן יכול לגבות אוטומטית כל ערב.

ואם יורשה לי, לרואים רחוק שבינינו...שיהיה לכם גיבוי אחד כזה רחוק ונסתר מהמחשב שלכם... שאם יפרצו לכם הביתה שלא יקחו גם את הגיבוי.

גיבוי נעים....