באגים בתוכנה הישראלית להחלפת קבצים המבוססת על דואר אלקטרוני

9 מרץ 2004 | דואר חשמלי | משה הלוי | halemo

החשיפה

ביום 8 מרץ 2004, במדור "חיים ברשת" באתר נענע, חשף אורן הוברמן את התוכנה הישראלית החדשה להחלפת קבצים. התוכנה החדשה נקראת "שר זה" ובאנגלית: Share Ze.

הכתבה באתר נענע על התוכנה החדשה
http://net.nana.co.il/Article/?ArticleID=105631&typeid=27&sid=10

הכתבה מספרת על שני בחורים ישראלים, צעירים בני 18, עתודאים, שעלו על רעיון מקורי להחלפת קבצים אנונימית מבלי שכתובת המחשב (כתובת ה IP) של מוריד הקבצים או משתף הקבצים תהיינה חשופות כלפי חוץ במאגר כלשהו או בשרת שמנהל את ההחלפות, שרת קלמנזון קום (kalmnazon.com).

אתר קלמנזון להורדת התוכנה
http://www.kalmanzon.com

הרעיון

הרעיון מאחורי שיטת החלפת הקבצים, הוא שימוש בשרתי דואר אלקטרוני שתומכים בפרוטוקולי דואר סטנדרטיים כמו pop3 לשליפת דואר ובפרוטוקול smtp למשלוח דואר. שימוש בדואר web המבוסס על שימוש בדפדפן המשתמש, אינו מתאים לתוכנה, ולכן אין להזין כתובות כאלו בתוכנה, כי התוכנה לא תעבוד.

המשמעות של שימוש בפרוטוקולי דואר pop3 ו smtp היא שניתן להשתמש בחשבון דואר שעובד עם תוכנות דואר אלקטרוני רגילות וסטנדרטיות כמו אאוטלוק אקספרס של מיקרוסופט או יודורה (Eudora) של חברת קוואלקום.

לתוכנה Share Ze, מגדירים את כתובת הדואר האלקטרונית של המשתמש, את כתובת השרתים, את השם ואת הסיסמה הנחוצים כדי לשלוף מכתבים. התוכנה ממליצה להשתמש בשירותי דואר אנונימי המספקים את התמיכה ב pop3 וב smtp, כמו hotpop וכדומה.

דואר אלקטרוני בחינם עם תמיכה ב pop3 ו smtp
http://www.hotpop.com

הבדיקה

בכתבה באתר נענע, ראיינו מומחה אבטחה אנונימי שבדק את התוכנה וקבע כי הרעיון מקורי ומעניין, אולם ישנן בעיות אחרות כמו חשיפת כתובות הדואר של המשתמשים, וירוסים שעלולים להישלח. מומחה האבטחה של נענע לא ציין דברים אחרים על פי הכתבה.

קראתי את הכתבה של אורן הוברמן, וגם אני הורדתי את התוכנה. התקנתי, הגדרתי, אתחלתי את המחשב, הפעלתי את המודם והתקשרתי שוב לרשת האינטרנט. הגדרתי לתוכנת קיר האש שלי (Fire Wall) שתאפשר לתוכנה החדשה לבצע תקשורות לרשת האינטרנט.

לפני שהפעלתי את התוכנה, הפעלתי את תוכנת הסניפר (sniffer) הצמודה שלי. תוכנת סניפר (רחרחן) היא תוכנה שבודקת איזה מידע יוצא לרשת האינטרנט מתוכנה כלשהי במחשב. כך ניתן לעקוב אחרי התוכנה החדשה ולראות שהיא לא עושה שטויות כמו לשלוח מידע החוצה לרשת שהיא לא אמורה לשלוח. כך למעשה מגלים האם תוכנה שהופצה באינטרנט להורדה, היא למעשה תוכנת ריגול או תוכנה שעושה רק את מה שהיא אמורה לעשות.

ואכן, על פי מספר בדיקות ראשוניות, התוכנה החדשה של הצעירים הישראלים אכן עשתה את המוטל עליה ולא יותר מכך. התוכנה אמינה ולא מרגלת או גורמת נזקים. עושה בדיוק את מה שהיא צריכה לעשות: לנהל החלפות קבצים.

דרך תוכנת הסניפר, תוכנה שנקראת CommView, ראיתי את הפקודות ששולחת התוכנה Share Ze לכיוון רשת האינטרנט, לשרת קלמנזון קום. חלק מהמידע אינו מוצפן כפי שטענו המפתחים, אלא מדובר בפקודות ידועות להבאת דפים משרת דפים באינטרנט (web server). הפקודות הן פקודות HTTP רגילות השולחות לשרת כתובת URL עם בקשה ופרמטרים. כולן פקודות GET של פרוטוקול HTTP.

מה שלכאורה מוצפן, הן התשדורות ששולחת התוכנה דרך הדואר האלקטרוני שהוגדר על ידי המשתמש. אילו הן מכתבים קצרים יחסית המכילים פקודות טקסט לחיפוש קבצים.

אופס, יש בעיות אבטחה

לאחר שניתחתי את התקשורות, והעתקתי לי אותן בצד, כיביתי את התוכנה. התוכנה סיימה את תפקידה. גם הסניפר סיים את תפקידו. בחלון של מעבד תמלילים פשוט, אפילו בתוכנת פנקס הרשימות (notepad) של מערכת ההפעלה חלונות, נרשמו הפקודות שנקלטו על ידי מקודם תוכנת הסניפר.

בבדיקה ראשונית מתברר כי גם כשהתוכנת Share Ze אינה פועלת על המחשב, ניתן לשלוט בשרת ובהחלפת הקבצים ואפילו לקבל מידע ולגרום למהומות אלקטרוניות שלא היו מתוכננות כלל על ידי כותבי התוכנה.

למרות שהתוכנה אינה פועלת, ניתן לקבל את רשימת האימיילים של המשתמשים כרגע בתוכנה, אותן כתובות דואר אלקטרוני שהוזנו זה מכבר לתוכנה. על פי הבדיקה, כאשר המשתמש מתנתק מן התוכנה, כתובת הדואר האלקטרוני שלו נמחקת מהרשימה הכללית והוא בעקרון אינו נמצא אונליין. כאשר הוא מפעיל את התוכנה, התוכנה שולחת את כתובת הדואר שלו לשרת של קלמנזון קום (kalmanzon.com),

קבלת כתובות האימייל של כל המשתמשים הרשומים בשרת, לכאורה משתמשים שכרגע נמצאים אונליין, היא פשוטה ומתבצעת על ידי מתן כתובת דף אינטרנט בשרת קלמנזון.

קישור מספר 1: זאת הכתובת לקבלת כל כתובות הדואר האלקטרוני
http://www.kalmanzon.com/ShareZEList/Public.txt

לחיצה על הקישור, תציג לכם בחלון הדפדפן אוסף של אותיות באנגלית בטקסט ארוך ולא מובן. מדובר על טקסט בקידוד סטנדרטי שנקרא base64.

כך למשל נראה הטקסט הלא ברור:

bmlzbnRAemFoYXYubmV0LmlsJCRob3N0ZmlsZXMxQGthbG1hbnpvbi5jb20kJGdhbGl0MjAwQGludGVybWFpbC5jby5pbCQkc2FtX2Zpc2hlckBCb25Cb24ubmV0JCRzYW1fZmlzaGVyQEJvbkJvbi5uZXQkJHNhbV9maXNoZXJAQm9uQm9uLm5ldCQkc2hhaTg1QG5ldHZpc2lvbi5uZXQuaWwkJG5zX3VsaWVsQGJlemVxaW50Lm5ldCQkYWl6aWtfbUBiZXplcWludC5uZXQkJGF6YXphejFASG90UE9QLmNvbSQkbm9ib2R5c3BlY2lhbEBib25ib24ubmV0JCRtYW51ZWxAaW50ZXJtYWlsLmNvLmlsJCR2ZWNzbGVyODdAaG90bWFpbC5jb20kJG9za2lAbmV0dmlzaW9uLm5ldC5pbCQkYmVrZXJAbmV0dmlzaW9uLm5ldC5pbCQkc2lnbGl0dEB3YWxsYS5jby5pbCQkbWFsZW5hX3JvbWFub0Bob3RtYWlsLmNvbSQkZml4eHhlcjZAQm9uQm9uLm5ldCQkZ3JuZG1zdHJAMDEyLm5ldC5pbCQkRW5kRW1haWxMaXN0

כדי לפענח מה כתוב, אנו זקוקים למפענח של קידוד base64. מפענח כזה קיים באינטרנט וכל מה שאנחנו צריכים זה לבחור זה אחד מתוך המון. אז הנה, בחרתי אחד.

קישור מספר 2: דף להמרת קידוד base64 לקידוד טקסט רגיל
http://www.toastedspam.com/decode64

הכניסו את הטקסט הגדול לעיל בחלון העריכה, ותקפידו ש pro או code יהיו מסומנים. לחצו על הלחצן decode, ואחרי מספר שניות, תקבלו בתחתית העמוד רשימת כתובות אימייל, מופרדות בשני סימני דולר $$.

אם תכניסו את הטקסט הגדול לעיל שקיבלתם על ידי הפעלת קישור מספר 1, תקבלו את הרשימה הבאה של כתובות דואר אלקטרוני:

nisnt@zahav.net.il$$hostfiles1@kalmanzon.com$$galit200@intermail.co.il$$sam_fisher@BonBon.net$$sam_fisher@BonBon.net$$sam_fisher@BonBon.net$$shai85@netvision.net.il$$ns_uliel@bezeqint.net$$aizik_m@bezeqint.net$$azazaz1@HotPOP.com$$nobodyspecial@bonbon.net$$manuel@intermail.co.il$$vecsler87@hotmail.com$$oski@netvision.net.il$$beker@netvision.net.il$$siglitt@walla.co.il$$malena_romano@hotmail.com$$fixxxer6@BonBon.net$$grndmstr@012.net.il$$EndEmailList

הוספת כתובת אימייל לרשימה

את רשימת כתובות האימייל לעיל, הכניסה לכאורה תוכנת החלפת הקבצים Share Ze. כל כתובת דואר הנמצאת ברשימה, מקבלת הודעות מהתוכנה בצורת משלוח של הודעת דואר אלקטרונית, ובהמשך ההודעה שנשלחה, נמחקת על ידי התוכנה של המשתמש שאמור להיות אונליין (כי כתובת הדואר שלו נמצאת ברשימה של המשתמשים הפעילים כרגע).

אבל, וזה באג השני (אם נחשיב כבאג ראשון את זה שכולם יכולים לצפות ברשימה), ניתן להכניס כתובת דואר אלקטרוני של אדם שאינו משתמש בתוכנה, אולי אפילו אחד שכלל לא הוריד אותה.

נניח שאנו רוצים להוסיף את בעל הכתובת koko@nospam.com.

כל שאנחנו צריכים הוא לעשות מה שהתוכנה עושה (כפי שקלטנו עם הסניפר מקודם), וזה לשלוח URL דרך הדפדפן, עם פרמטר אחד שמציין את כתובת האימייל של הקורבן.

קישור מספר 3: הוספת כתובת אימייל של הקורבן
http://www.kalmanzon.com/ShareZEList/listmanger.php?Fucntion=AddEmail&GroupName=Public&EmailAddr=koko@nospam.com

כך הכנסנו לרשימה כתובת של קורבן שאינו משתמש בתוכנה. מה שיקרה הוא שהקורבן יקבל דואר זבל עם כל הפקודות של מחפשי הקבצים שמשתמשים בתוכנה כרגע ונמצאים אונליין.

מכיוון שהקורבן אינו משתמש בתוכנה, כתובת הדואר האלקטרונית שלו לא תימחק והוא יקבל צרורות של מכתבים קצרים שהתוכנה שולחת גם לו, בנוסף למשתמשים המחוברים.

מחיקת כתובת אימייל מהרשימה

באג שלישי הוא האפשרות למחוק כתובות דואר אלקטרוני מהרשימה. גם כתובות של משתמשים אונליין שמשתמשים בתוכנה. כל שצריך הוא להפעיל את ה URL המתאים, כפי שקלטנו אותו בסניפר.

נניח שאנו רוצים למחוק את בעל הכתובת koko@nospam.com.

שוב, כל שאנחנו צריכים הוא לעשות מה שהתוכנה עושה (כפי שקלטנו עם הסניפר מקודם), וזה לשלוח URL דרך הדפדפן, עם פרמטר אחד שמציין את כתובת האימייל של הקורבן שברצוננו למחוק.

קישור מספר 4: מחיקת כתובת אימייל של הקורבן:
http://www.kalmanzon.com/ShareZEList/listmanger.php?Fucntion=RemoveEmail&GroupName=Public&EmailAddr=koko@nospam.com

כך נוכל למחוק משתמשי תוכנה בזמן אמת, והם לא ידעו מדוע הם לא מקבלים קבצים או הודעות של מחפשי קבצים אחרים.

דוגמה להודעת זבל שנשלחת לקורבן

רישום כתובת אימייל של הקורבן, תגרום לו לקבל הודעות לא רצויות ששולחת התוכנה המופעלת על ידי משתמשים אונליין בתוכנה.

כך נראית הודעה שנשלחת לקורבן על ידי התוכנה:

כתובת השולח תהיה (From):
Hello Share Search

שורת הנושא תהיה (Subject):
6659554A501C6E7D1865595411157A5D5055675D54435750111571565162515651

ותוכן הודעה תהיה:
<$SCommand$>6654554A565972515954$$CCDDDADC$$5150465C544205787D5E40687A611A5B5A5C$$0$$0$$0$$03030409$$EndData<$SCommand$>

סוף דבר

תוכנת Share Ze נראית נחמד, אבל הרעיון שעומד מאחוריה הוא לא טוב. שימוש בדואר אלקטרוני כדי להחליף קבצים בצורה שבה התוכנה עובדת, גורם להתגברות של דואר זבל ולקורבנות לא רצויים.

הצפנה של מסרים אינה מספיקה, ויש לבנות את התוכנה בצורה כזו שאחרים לא יוכלו להעתיק ולדמות את התקשורות שלה לרשת האינטרנט.

שאלות נוספות יש להפנות למומחה האבטחה של אתר נענע ;-).

~~~~~~
http://halemo.net
~~~~~~