

May 2001

תולעת הפוגעת בשרתי Solaris ו- IIS השחיתה עד כה כ- 8800 אתרי אינטרנט

ב- 8 במאי, נשלח לארגון האבטחה Attraction.org מידע לגבי ווירוס מסוג תולעת המכונה Sadmind/ISS. המידע כלל 8800 כתובות של אתרי אינטרנט שנפלו קורבן לתולעת, לטענת מפיציה. מבדיקה שנערכה על ידי הארגון עולה כי הרשימה מהימנה בחלקה הגדול.

התולעת מנצלת חור אבטחתי ידוע בתוכנת הניהול Solstice sadmind במערכת ההפעלה סולריס עד גרסה 7. לאחר מכן היא מנצלת את מערכות הסולריס הפגועות כדי לתקוף דרכן מערכות סולריס נוספות. כאשר התולעת מאתרת שרת IIS עם חור אבטחתי ישן שהתגלה לפני כחודשיים בשרתי IIS של מיקרוסופט, היא מנצלת אותו ומחליפה את הדף הראשי של האתר בדף משלה עם כתובות נאצה אנטי אמריקאיות. יש לציין שמדובר בשתי פרצות אבטחה ידועות; Sun הודיעה על תיקון לפרצת ה- Sadmind לפני למעלה משנתיים ואילו מיקרוסופט פרסמה טלאי אבטחה לשרתיה לפני קרוב לשנה. טלאי אבטחה ממיקרוסופט:

<http://www.microsoft.com/technet/security/bulletin/MS00-078.asp>

עבור שרתי סולריס:

<http://access1.sun.com/>

באג אבטחתי חמור התגלה בשרת ה- IIS 5 של מיקרוסופט

באג אבטחתי חמור התגלה בשבוע שעבר במערכת IIS 5 מתוצרת חברת Microsoft. הבאג התגלה ע"י חברת eEye.com שגם שרת ה- IIS שלה נפל קורבן לתקיפה מוצלחת לפני מספר חודשים.

באג זה מאפשר לפורץ פוטנציאלי קבלת גישה ויכולת להפעיל קוד תוכנה על גבי שרת Web מרחוק דרך פרוטוקול http. שרון בסר, CTO של חברת קומסק-פבליקום, הוסיף כי "מאחר והתקיפה מופעלת בגישת http, מערכות firewall אינן יכולות להגן מפניה ללא תמיכה בסינון תוכן מתאים או שימוש במערכת אבטחה משלימה כגון AppShield מתוצרת חברת Sanctum".

בסר ממליץ על מספר צעדים אשר יש לנקוט באופן מיידי: התקנת patch של מיקרוסופט, מייד לאחר מכן הקשחת השרת והסרת תוכנות לא רצויות, ביצוע code review, בחינת האפליקציה, וסינון תוכן באמצעות AppShield. את ה- patch ניתן להוריד ב-

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29321>

חברת קומסק-פבליקום מתמחה בבדיקת אפליקציות ושירותי אינטרנט ומפיצה את מוצרי Sanctum להגנת תוכן באתרי אינטרנט.

דבר המערכת

שלום רב לכל קוראינו, במהדורה הנוכחית של ה- Secur-eTon עדכונים חמים בתחום אבטחת המידע, סקירה על אבטחת המידע בתחום הפיננסי וכתבה ראשונה בסדרת כתבות בנושא ה-PKI.

קריאה נעימה,
צוות העיתון וחברת
קומסק-פבליקום

תוכן

עמוד 1	חדשות
עמוד 2	סקירת PKI
עמוד 3	כנס בנקאות
עמוד 3	טיפ שבועי

secureton@comsec.co.il

קדיטים

כתיבה: רווית גרייצר, גיל פונדיק

ייעוץ טכנולוגי: שרון בסר

עריכה: אמיר קראוס



תשתית מפתחות ציבוריים (PKI)

רוגן, יצפין בעזרתו הודעה וישלח לרוגן. רוגן שיקבל את ההודעה יפענח אותה בעזרת המפתח הפרטי שלו.

לתעודות ספרתיות שני תפקידים עיקריים:

הן מאשרות שהמחזיקים בהן – אנשים, אתרי אינטרנט, ואפילו משאבי רשת כגון נתבים – הם אכן מי שהם טוענים.

הן מגנות על מידע מקוון מפני השחתה או זיוף

(Data Integrity).

2. הצפנת מפתחות ציבוריים ופרטיים (הצפנה אסימטרית).

תשתית מפתחות ציבוריים מבוססת על הצפנת מפתחות ציבוריים שהיא השיטה הנפוצה ביותר כיום לזיהוי שולח הודעות או הצפנת הודעות על גבי האינטרנט. ההצפנה הסימטרית המסורתית הייתה מבוססת על יצירת מפתח סימטרי (הידוע הן לשולח והן למקבל) המשמש הן עבור הצפנה והן עבור פענוח.

החסרון העיקרי של שיטה זו נעוץ בעובדה שאם משתמש מסוים מצליח לפענח את המפתח, ניתן בקלות לפענח את הודעות המוצפנת בעזרתו. לעומת זאת, השיטת ההצפנה האסימטרית עליה מבוססת תשתית ה-PKI, המפתח הפרטי והמפתח הציבורי נוצרים בו זמנית תוך שימוש באותו אלגוריתם (RSA למשל הוא אלגוריתם פופולארי), המפתח הפרטי ניתן רק למשתמש ואילו המפתח הציבורי מתפרסם כחלק מתעודה ספרתית ב-directory אליו יכולים כל המשתמשים להיכנס. המשתמש אינו מתחלק במפתח הפרטי שלו עם משתמשים אחרים ומקבל אותו באופן מאובטח ואישי.

3. רשויות התעדה. רשות התעדה (CA) היא המקבילה הדיגיטאלית למשרדי הנפקת דרכונים. רשויות אלה מוודאות עם רשויות הרישום שהמידע שסופק ע"י מבקש התעודה אכן נכון, טרם הנפקת התעודה. רשות התעדה לוקחת את המפתח הפרטי של משתמש או ארגון, משלבת אותו עם מידע מזהה אחר, מכניסה אותו לתעודה הספרתית ואז "חותמת" אותו באופן מוצפן באופן שאינו מאפשר הכנסת שינויים (פונקציית hashing).

4. רשויות רישום. רשויות רישום משמשות כמתווך בין המשתמש לרשות ההתעדה ומוודאות שהמשתמש הוא אכן מי שהוא טוען טרם מפיקה רשות ההתעדה תעודה ספרתית.

PKI היא אחת מהטכנולוגיות המדוברות ביותר כיום בעולם המיחשוב ואחת ההבטחות הגדולות ביותר בתחום הזיהוי והאבטחה. עם העברתו של חוק החתימה הדיגיטלית בכנסת והחלתו בספטמבר השנה, מקבל הנושא תוקף מעשי.

כתבה זו הינה הראשונה מבין מספר כתבות שיתמקדו בנושא ובה נסביר מהי תשתית מפתחות ציבוריים וכיצד היא עובדת. בגיליונות הבאים נדון ביתר הרחבה בנושא ההצפנה, חתימה דיגיטלית, ההבדלים בין יצירת תשתית PKI עצמאית ורכישת שירותים כוללים וכן נסקור את היבטי האבטחה של מערך ה-PKI כחלק מ-Windows 2000. Stay tuned.

PKI היא תשתית מפתחות ציבוריים (לפעמים נקראת גם הצפנה אסימטרית) המאפשרת למשתמשי רשת ציבורית שאינה בטוחה מטבעה, כדוגמת האינטרנט, להחליף מידע וכסף באופן פרטי ומאובטח באמצעות שימוש בזוג מפתחות הצפנה, האחד פרטי והאחר ציבורי, המונפק ונשמר ע"י צד שלישי מהימן – רשות התעדה. רשות זו מספקת תעודות ספרתיות שתפקידן לזהות אדם או ארגון ושירותי directory לצורך שמירה על התעודות ובמקרה הצורך, אף ביטולן.

תשתית PKI מורכבת מכמה חלקים:

1. תעודות ספרתיות (digital certificates)
2. הצפנת מפתחות ציבוריים ופרטיים
3. רשויות התעדה (certificate authorities)
4. רשויות רישום (registration authorities)

1. תעודות ספרתיות. תעודה ספרתית היא מסמך אלקטרוני המשמש כמעין דרכון מקוון המזהה את בעליו על גבי רשת האינטרנט. מסמך זה המונפק ע"י רשות התעדה, מכיל את השם הפרטי של בעליו, מספר סידורי, תאריך תפוגת המסמך, עותק של המפתח הציבורי של בעל הכרטיס (המצוי ממילא ב-directory ציבורי כלשהו) וחתימה דיגיטאלית של הרשות שהנפיקה את המסמך כדי שמקבל המסמך יוכל לוודא שהמסמך מקורי. תעודות ספרתיות נשמרות בד"כ ב-directories כדי שמשתמשים יוכלו לחפש מפתחות ציבוריים של משתמשים אחרים. כך למשל, אם דני רוצה לשלוח הודעה מוצפנת לרוגן, הוא יפנה ל-Directories ציבורי, יחפש את המפתח הציבורי של

חברת קומסק-פבליקום עוסקת ביעוץ והקמת מערכות תשתית PKI תוך התמקדות בבחינת הצרכים והשלבים השונים של תהליך ההטמעה.



טיפ שבועי

"אבטחת מידע במערכות בנקאיות ופיננסיות" – רשמים מכנס

על מנת לשפר את ביצועי ה-VPN Gateway מומלץ להשתמש בכרטיס מאיץ VPN (VPN Accelerator)

מהו מאיץ VPN?

מאיץ VPN הוא כרטיס תואם PCI המגביר את יכולות התפוקה של ה-VPN-1 Gateway. הכרטיס כרגע מגיע בשתי גרסאות: מאיץ VPN, מאיץ VPN II.

מהן היכולות של המאיץ?

מפחית מהעומס המופעל על ה-CPU; מגביר את תפוקת ה-VPN-1 Gateway ל-100Mbps; תומך בפרוטוקולי IPSec/IKE.

מהו שוק היעד עבור המוצר?

התקנות VPN-1 3DES עם דרישות לביצועים גבוהים (מספר רב של חיבורי אינטרנט T1/E1); התקנות VPN-1 שבהם משאבי ה-CPU מנוצלים באופן מקסימאלי. ניצול מקסימאלי של CPU עשוי לנבוע מ-CPU מוגבל (P1, K6 וכו'), או בשל gateway המבצע מספר משימות אבטחה בו-זמנית כגון VPN, firewall, שרתי אבטחה, NAT וכו'.

מהם היתרונות ללקוח?

מגביר תפוקה מקסימאלית של VPN-1 gateway; עובר 45Mbps עבור מאיץ VPN; 100Mbps עבור מאיץ VPN II; משחרר משאבי CPU לצורך ביצוע פעולות נוספות; משתלב בקלות עם VPN-1 מבית צ'ק פוינט.

לאיזה פלטפורמות מתאים המאיץ?

ניתן להתקין כרטיסי מאיץ עבור מערכות NT, Solaris, ו-Nokia Appliances. למערכות בעלות CPU נוסף, קיים גם פתרון תוכנה המתאים לתצורה.

מאיצי VPN קיימים עבור מגוון מוצרי VPN בשוק; מוצרי צ'ק פוינט, סיסקו ואחרים. לכל מוצר המאיץ התואם.

חברת קומסק-פבליקום ערכה ב-24 לאפריל כנס למגזר הבנקאי והפיננסי שעסק בהיבטים השונים בתחומי אבטחת המידע והצרכים היחודיים של המערכות הפיננסיות בתחום. אורח הכבוד היה מר איתן לוברוסו, סגן נשיא בכיר בבנק צייס מנהטן. לוברוסו הציג מגמות עולמיות בתחומי הבנקאות וסקר את התוכניות האסטרטגיות של הבנקים בעולם להחדרת שירותים חדשים, תוך חיבור המערכות הרגישות לרשת האינטרנט.

EBPP & Electronic Bill Presentment

הינו שירות חדש, בו כל אחד מלקוחות הבנק יוכל להיכנס לאתר אינטרנט מרכזי אחד ולראות את כל יתרות חשבונותיו גם בבנקים האחרים כמו גם יתרות התשלום מול כל חברות השירותים איתם הוא עובד כדוגמת בזק, חברת חשמל וכו', ולשלם את חשבונותיו דרכו. מהלך כזה הוא בבחינת פריצת דרך משמעותית שכן הוא מקל ומקצר עבור הצרכן תהליכים רבים, אך טומן בחובו בעיות אבטחת מידע רבות. פגיעה או פריצה לאתר מרכזי שכזה יכולה לאפשר גישה מיידית לכל חשבונות הלקוחות במערכות הבנקאיות וחברות השירותים המקושרות אליו.

בתקופה הקרובה עתידים הבנקים להציע גם אספקת שירותים בנקאיים מלאים לא רק באמצעות המחשב האישי, אלא אף באמצעות מכשירים נישאים כגון PDA למיניהם וסלולר. הבעייה המרכזית באספקת שירותים מסוג זה היא החיבור הבעייתי של המערכת הבנקאית לרשתות הסלולר ואויר אלחוטיות מעבר לחיבור לרשת האינטרנט. התקשורת דרך רשתות אויר פותחות אפיקים נוספים לפריצה ויירוט הטרנזקציות הכספיות ונחשבות למסוכנות וחשופות הרבה יותר מאשר תקשורת דרך מערכות אינטרנטיות. נפיצותו של שירות זה ע"י המערכת הבנקאית וההתפתחויות הטכנולוגיות בתחום זה תלויים בעיקר במידת אימוץ השירות בקרב הצרכן הסופי. המבחן האמיתי יהיה האם באמת הצרכנים השונים ירצו לבצע טרנזקציות כספיות דרך הסלולר, דבר שיחייב את המערכת הבנקאית לספק שירות זה בצורה המאובטחת יותר.

