

July 2001

יצרני תוכנות אנטי וירוס מזהירים נגד וירוס קטלני המכונה Sircam

יצרני תוכנות אנטי מזהירים מפני וירוס המופץ באמצעות דואר אלקטרוני מבוסס Windows המכונה Sircam. וירוס זה מסוגל באופן פוטנציאלי למחוק קבצים המצויים על הדיסק הקשיח או לגרום לקריסת המחשב.

Sircam הוא וירוס המגיע עם קבצים מצורפים (attachments) המבקש מקורבנות תמימים – באנגלית או בספרדית – לפתוח מסמך מצורף ואז הוא פוגע במחשב. למרות ש-Sircam אינו פוגע באופן עקיב בכל מחשב אליו הוא מגיע, הוא עלול ליצור קובץ חדש בדיסק הקשיח שלו כדי למלא אותו ולגרום לקריסתו, או פשוט למחוק את כל הקבצים על גבי המכונה. כוירוס הממען את עצמו תוך שימוש ב-Outlook directory של הקורבן, הוא מסוגל גם להסב נזק עצום לשרתי דואר אלקטרוני.

Sircam שונה מוירוסים אחרים המופצים באמצעות דואר אלקטרוני כגון Anna Kournikova בכך שהוא למעשה תוכנת Windows המסוגלת להפש קבצים בדיסק הקשיח, לרבות קבצי Excel, קבצי Zip או קבצי הרצה ואז לצרף אותם לקובץ המצורף שהוא שולח. ה"תוספת" הזו אינה נראית כקובץ מצורף שני, אלא פשוט מגדילה את הקובץ המקורי. תכונה בלתי שגרתית נוספת היא היכולת שלו לבחור בשורת נושא (subject line) שרירותית שהיא למעשה זהה לשם הקובץ המצורף. כדי להסיר את הוירוס, יש למחוק קבצים מסוג w32.sircam.Worm@mm וכן למחוק אותו מקובץ ה-Autoexec.bat. כמו כן יש לשנות בחזרה את ה-registry key HKEY_CLASSES_ROOT\exefile\shell\open\command למידע נוסף

<http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html>

וירוס המכונה Code Red תוקף

אתרים ברחבי העולם

קוד אדום, וירוס אינטרנטי חדש מסוג תולעת משהית אתרים דוברי אנגלית ומציג בדף הבית שלהם את המשפט "Welcome to Hacked By Chinese! http://www.worm.com!". הוירוס מנצל פרצה ידועה בשרת ה-IIS של מיקרוסופט הקשורה לקבצי .ida ו-.idq עבודה שחזרה מיקרוסופט טלאי אבטחה זה מכבר אולם אתרים רבים, לרבות אתר ה-Windows Update של מיקרוסופט עצמה לא התקינו אותו.

על האתרים שנפרצו נמנים אתר הבית הלבן, אתרי מיקרוסופט ועוד. נראה כי התולעת נותנת הוראה למחשבים הנגועים לצאת במתקפת מניעת שירות (Denial of Service) על אתרים, בדומה למתקפה שהפילה את אתרי יאהו! ו-eBay בפברואר בשנה שעברה. בנוסף למתקפת מניעת שירות שמשתקת אתרים ע"י מניעת אפשרות לענות לבקשות לגיטימיות, מסוגל הוירוס גם להאט באופן משמעותי תעבורת אינטרנט ע"י הצפת אתרים בתעבורת מסרים ממחשבים נגועים. ההערכה היא כי כ-12,000 מחשבים ברחבי העולם כבר נדבקו בתולעת הקוד האדום.

דבר המערכת

שלום רב לכל קוראינו, במהדורה הנוכחית של ה-Secur-eTon חדשות טריות בתחום אבטחת מידע, כתבה שלישית (ואחרונה) בנושא PKI, וסקירת תוכנת PrivateArk מבית CyberArk. קריאה נעימה, צוות העיתון וחברת קומסק-פבליקום

תוכן

עמוד 1	חדשות
עמוד 2	PKI - כתבה 3
עמוד 3	זרקור על מוצר

secureton@comsec.co.il

קדיטים

כתיבה: רווית גרייצר, גיל פונדיק

ייעוץ טכנולוגי: שרון בסר

עריכה: אמיר קראוס



6 שלבים לפריסת תשתית מפתחות ציבוריים (PKI)

(כתבה אחרונה בסדרה)

- רכישת חומרה ותוכנה – הגורמים אותם יש להביא בחשבון הם סביבת העבודה הקיימת, מוצרי התוכנה/חומרה אותם מכיר צוות הפרויקט, רמת הסקלאביליות של המוצרים וכדומה.

שלב 3: פיתוח ובדיקה

מטרת שלב זה להבטיח שכל התוכנות הנדרשות או כל בדיקה של רכיבי המערכת יעשו טרם התקנת ה-PKI. כמו כן, יש לעשות סקר סיכונים מחודש בלתי תלוי שיבחן את נקודות החולשה של המערכת המוצעת ויציע הצעות לתיקון. במקביל יש להכשיר את הצוות התפעולי, רשויות הרישום וה-help desk בכלל הנוגע לניהול פתרון ה-PKI הנבחר.

שלב 4: התקנה, אינטגרציה ובדיקת המערכת

בשלב זה מותקנים כל רכיבי תשתית ה-PKI בארגון לרבות:

- התקנת רשת, firewall, חומרה, מערכות הפעלה ותוכנות צד שלישי.
- התקנת Directory ותוכנת Web.
- התקנת תשתית ה-PKI מהיצרן שנבחר ע"י הארגון (Baltimore, Entrust וכו') וחומרה תומכת.
- שילוב עם מערכות קיימות.
- בדיקת כל היבטי המערכת.
- תיעוד המערכת.

שלב 5: ביצוע פיילוט

במסגרת הפיילוט נבחן השימוש ב-PKI באמצעות מספר משתמשים מצומצם בסביבה מבוקרת. הפיילוט אמור להימשך בין ארבעה לשישה שבועות ובמידה והוא מצליח יש להכניס את המערכת לשימוש באופן הדרגתי ליתר המחלקות בארגון. מומלץ להפיץ עלון פנימי ובו להסביר לקבוצת הפיילוט על השינויים הכרוכים בהכנסת תשתית ה-PKI. קבוצת הפיילוט יכולה לנוע בין 50 ל-500 משתמשים. חשוב לבחור באנשים בעלי מודעות גבוהה ופתיחות שיהיו "שגרירים" טובים של הנושא ליתר משתמשי הארגון. כמו כן יש לתעד באופן מסודר את ממצאי הפיילוט. טרם ההתקנה הכוללת, יש להביא בחשבון שני גורמים חשובים: הפצת תוכנה בצד הלקוח ויצירת משתמשים.

(המשך בעמוד 3)

לאחר שסקרנו טרמינולוגיית PKI בסיסית, התוודענו לרכיבי המערכת ולאופן בו עובדת הצפנה העומדת בבסיס חילול המפתחות, אנו מציעים לכם שיטה בת 6 שלבים לפריסת תשתית PKI ארגונית.

שלב 1: ייזום הפרויקט ותכנונו

בדומה לכל פרויקט IT אחר, גם הטמעת PKI צריכה להיות מתוכננת ומבוצעת בקפידה. ראשית, יש להציב מטרות ולפתח אסטרטגיה להשגתן. מספר שאלות חשובות שעל כל ארגון לשאול את עצמו לפני שהוא מתחיל ביישום PKI הן לשם מה הוא זקוק לתשתית זו, האם היא מיועדת לשימוש פנימי או חיצוני, כיצד תוביל הטמעת תשתית PKI להיסכון בעלויות ועוד. כאן המקום להציג את התוכנית בפני ההנהלה הבכירה ולמנות את צוות הפרויקט. יש להחליט האם הצוות יורכב מאנשי הארגון או יעשה ב-outsourcing, לקבוע את מספר המשתמשים העתידיים הן עבור הפילוט והן עבור היישום עצמו וכן לכתוב תוכנית מסודרת הכוללת זמני יעד.

שלב 2: ניתוח דרישות ועיצוב

טרם בניית התשתית, חשוב להבהיר על אילו דרישות נועדה המערכת לענות כגון:

- האם על המערכת לספק אבטחה, תקינות מידע, אי הכחשה או כל אלה גם יחד?
- מהי מדיניות האבטחה המתוכננת?
- מהי פלטפורמת החומרה המיועדת?
- האם יש מערכות legacy איתם צריך להשתלב?
- בשלב זה יש לקבל החלטות לגבי המשאבים שיוקצו לטובת הפרויקט לרבות:
- ניתוח, עיצוב ותיעוד מדיניות התעודות הדיגיטאליות
- קיום פגישות עם כל אחת מן המחלקות בארגון בנושא חשיבות נושא ה-PKI ומדיניות אבטחה כלל ארגונית.
- עיצוב ארכיטקטורת מערך ה-PKI לרבות רשויות הרישום וההתעדה, directory ועוד.
- בחירת צוות ניהול הפרויקט (מפתחים, אדמיניסטרטורים ועוד).



זרקור על מוצר

PrivateArk Network Vault

PrivateArk היא תוכנה פרי פיתוחה של חברת CyberArk, חברה ישראלית שהוקמה ב-1999, המאפשרת לארגונים ליצור "כספות רשת" ייעודיות. כספות אלה הם למעשה שטחי אחסון מאובטחים, הנגישים למשתמשים דרך ה-LAN, WAN או האינטרנט. חדרי כספות אלה מקנים אבטחת קבצים רגישים ושרתי קבצים, הגנה על תוכן אינטרנטי רגיש ועל מאגרי נתונים ועסקאות e-business, אגירת מסמכים החתומים בחתימה דיגיטלית לטווח הרחוק ועוד.

הרעיון העומד בבסיס הכספת גורס כי כשם שבני אדם לא הופכים את ביתם למבצר כדי להגן על מספר חפצים יקרי ערך, כך גם המשתמש ברשת אינו מעוניין לבצר את הרשת כולה, שיטה היוצרת סרבול מיותר ומקשה על העבודה השוטפת. PrivateArk מבוססת למעשה על רעיון הכספת הבנקאית, שבה יכולים משתמשים לאחסן בכספת הרשת מידע רגיש כדוגמת קבצים, עסקאות אלקטרוניות, מאגרי נתונים, הודעות דואר אלקטרוני, תוכן אינטרנטי וסיסמאות. בדומה לכספת בבנק הממוגנת היטב, כך גם תוכנת PrivateArk ממגנת את עצמה במספר שכבות אבטחה לרבות רשתות וירטואליות פרטיות (VPN), firewall, בקרת גישה, אותנטיקציה, הגנה מפני וירוסים והצפנה.

התוכנה מותקנת על שרת נפרד ברשת (NT או Windows 2000) ומבוססת על ארכיטקטורת שרת/לקוח על פיה מוגדר מאגר משתמשים מורשים. כל משתמש חייב להיות מזוהה טרם כניסתו לכספת וברגע שאושרה כניסתו הוא מקבל זכויות כפי שנקבע לו ע"י מנהל הרשת. כל המידע בתוך הכספת אגור ומוצפן בתוך כספות קטנות. PrivateArk מאפשרת לכל מחלקה בארגון לאבטח את המידע הרגיש שלה ולהגדיר מראש מי רשאי לגשת לאילו קבצים בכספות השונות. לדוגמא, ניתן לקבוע שכל העובדים במחלקת כוח אדם יורשו לגשת לקבצי משכורות עובדים אולם רק למנהל כוח אדם יותר לשנות או למחוק אותם.

אחת התכונות המעניינות של התוכנה היא אבטחה חזותית - באמצעות feature זה יכולים משתמשים ומנהלי רשת לדעת מייד על כך שמישהו ניגש לכספת, עדכן או הוסיף אובייקטים או כל פעולה אחרת שנעשתה בכספת. מנהלי רשת אף יכולים לראות מי היה המשתמש האחרון שנכנס לכספת. בקרה חזותית מסוג זה מגבירה את המודעות לאבטחה וכן מונעת מעובד שיעזוב או יפטר מלגשת לסודות חברה שכן רישומי היסטוריית הנכנסים לכספת יסגירו אותו.

6 שלבים לפריסת PKI - המשך מעמ' 2 -

הפצת תוכנת לקוח:

הפעלת מערכת ה-PKI כוללת הפצת תוכנה בצד המשתמש. היות שתוכנות אלה נוטות להיות מורכבות ובעלות נפח הגדול מדיסקט 3.5, מומלץ לשקול דרכי הפצה שונות כגון התקנת התוכנה על גבי שרת מרכזי עבור התקנה ישירה, הורדת התוכנה מאתר אינטרנט או צריבתה על גבי CD-ROM. ההמלצה היא לעשות את מרבית עבודת הקונפיגורציה של התוכנה בחבילת ההפצה (מרבית הספקים מצרפים כלי המאפשר לעשות זאת) במטרה למנוע עד כמה שניתן התערבות מצד המשתמש הסופי ולפשט את התהליך.

יצירת משתמשים:

זהו תהליך המורכב משלושה שלבים: אתחול משתמשים, shared secret (הכולל הפצת מספר רישום וקוד הרשאה) ורישום משתמשים.

אתחול משתמשים (initialization) – ניתן לאתחל משתמשים ע"י הכנסת פרטי המשתמש באופן ידני או לעשות זאת באופן אוטומטי שבו מאגר נתוני משתמש מועלה באופן סיסטמטי למערכת ה-PKI (נחוץ במקרים בהם מדובר במספר רב של משתמשים).

Shared secret – לאחר אתחול המשתמשים, מקצה מנהל המערכת למשתמש מספר רישום (shared secret reference number) וקוד הרשאה.

רישום משתמשים - בשלב זה תחולל תוכנת הלקוח את זוג המפתחות של המשתמש ותשלח את המפתח הציבורי למערכת ה-PKI.

שלב 6: תפעול ותחזוקה

בתום ההתקנה, יש להבטיח תפעול שוטף ותחזוקה לרבות:

- ניהול משתמשי קצה
- בדיקת קבצי הלוג של המערכת
- גיבויי מערכת ואיסוף נתונים על פעולת המערכת
- בקרה
- איסוף תגובות משתמשים ועוד.

*המאמר מבוסס על נייר עבודה של חברת Entrust ועל ניסיון שהצטבר בקומסק בתחום.