OUCH! מאי 2014

הניוזלטר החודשי למודעות אבטחת מידע למשתמשי המחשב

OUCH!

בגליון זה...

- סקירה
- אינדיקציות לפריצה
- איך להגיב

פרצו אלי, מה עכשיו?

סקירה

אנו יודעים שאתם מודאגים בנושא הגנה על המחשב והמידע שלכם ושאתם נוקטים בצעדים על מנת להגן עליהם. עם זאת, כמו בנהיגה במכונית, לא משנה כמה בטוח אתם נוהגים, במקודם או במאוחר אתם עלולים להיות מעורבים בתאונה. בניוזלטר זה אנו נלמד אתכם מה לחפש על מנת לקבוע אם מחשבכם התוקף, ואם כן, מה לעשות בנדון. לבסוף, ככל שתזהו שהמחשב שלכם הותקף, וככל שתגיבו במהירות, כך תפחיתו בצורה הטובה ביותר נזק כלשהו לכם או לארגון שלכם.

עורך אורח

ג'ייק ויליאמס (Jake Williams; @MalwareJake; malwarejake.blogspot.com) הוא המדען הראשי ב – CSRGroup ייעוץ אבטחת מחשבים. הוא הכותב המשותף של קורסי SANS (Memory Forensic (FOR 526 ו .Malware (Reverse Engineering (FOR 610-

אינדיקציות לפריצה

דבר ראשון אתם צריכים להבין שאין צעד בודד בו אתם יכולים לנקוט על מנת להחליט האם המחשב שלכם נפרץ. במקום זה יש בדרך כלל מספר אינדיקציות. אם אתם מזהים שילוב של אינדיקציות אלו, ניתן להניח שהמחשב שלכם נפרץ. להלן מספר דוגמאות:

- מערכת האנטי וירוס במחשב שלכם הקפיצה התרעה שהמחשב שלכם נגוע, במיוחד אם היא מתריעה שהיא לא יכולה להסיר או להעביר להסגר את הקבצים הנגועים.
- דף הבית של הדפדפן שלכם השתנה באופן בלתי צפוי או שהדפדפן לוקח אתכם לאתרים שאינכם מעוניינים לצפות בהם.
- יש במחשב שלכם חשבונות חדשים שלא אתם יצרתם.
- תכניות חדשות רצות במחשב מבלי שהתקנתם אותן.
- המחשב שלכם קורס פעמים רבות או עובד מאוד לאט.
- תכנית במחשב שלכם מבקש אישורכם לערוך שינויי מערכת, למרות שאינכם מתקינים או מעדכנים אף אחד מהיישומים שלכם.
- הפיירוול מתריע שתוכנית שאתם לא מכירים מבקשת הרשאות לגשת לאינטרנט.

© The SANS Institute 2014

פרצו אלי, מה עכשיו?

איך להגיב

במוקדם או במאוחר המחשב שלכם עלול להיות מותקף. ככל שתזהו זאת מוקדם יותר, ותטפלו בכך מהר יותר, כך המצב שלכם יהיה טוב יותר.

אם אתם חושבים שהמחשב שלכם נפרץ, ככל שתגיבו מוקדם יותר כך המצב יהיה טוב יותר. אם המחשב שאתם משתמשים בו סופק ע»י המעסיק שלכם או משמש אתכם לצרכי עבודה, אל תנסו לתקן את המחשב בעצמכם ואל תכבו את המחשב. לא רק שלא תועילו בכך, אלא שאתם עלולים להרוס ראיות חשובות שעשויות להיות שימושיות בחקירת האירוע. במקום זאת, דווחו על האירוע למעסיק שלכם באופן מידי, בדרך כלל באמצעות פניה לתמיכת המחשבים של החברה (Help Desk) או גוף אבטחת המידע (חמ»ל סייבר). אם מסיבה כלשהי אתם לא יכולים ליצור קשר עם מקום העבודה שלכם, או שאתם חוששים מעיכוב בטיפול באירוע, נתקו את המחשב שלכם מהרשת והעבירו אותו למצב השהיה או שינה (sleep/ suspend / hibernate). גם אם אתם לא בטוחים שהותקפתם, עדיף לדווח על כך באופן מיידי, על כל צרה שלא תבוא. לארגון שלכם יש בוודאי נהלים לטפל באירועים כאלו, ולכן עדיף לתת לארגון לטפל במקרה כזה.

אם המחשב הוא רכושכם ולשימושכם האישי הנה מספר צעדים שאתם יכולים לנקוט בעצמכם:

- **גיבויים** – המהלך החשוב ביותר שאתם יכולים לעשות הוא להתכונן מבעוד מועד עם גיבויים. גבו את המידע שלכם באופן קבוע ומדי פעם בדקו שאתם יכולים לשחזר את המידע. לעיתים קרובות כאשר מחשב מותקף, האפשרות היחידה שיש לכם היא למחוק את המערכת מהדיסק הקשיח ולהתקין מחדש את מערכת ההפעלה או לרכוש מחשב חדש. בשני המקרים אתם זקוקים לגיבויים שלכם על מנת לשחזר את המידע האישי שלכם.
- **שינוי סיסמא** – וודאו כי שיניתם את כל הסיסמאות שלכם. זה כולל לא רק את הסיסמאות על המחשב והמכשיר הנייד שלכם, אלא כל הסיסמאות המקוונות שלכם. וודאו שאתם משנים את הסיסמאות ממחשב אחר שניתן לסמוך על כך שהוא בטוח.
- **אנטי וירוס** – אם האנטי וירוס שלכם מתריע לכם על קובץ נגוע, אתם יכולים לעקוב אחרי ההוראות שהוא נותן לכם. זה בדרך כלל כולל העברת הקובץ להסגר, ניקוי הקובץ או מחיקת הקובץ. מרבית מערכות האנטי וירוס יכילו קישורים שאתם יכולים לעבור אליהם וללמוד לגבי הנוזקה שתקפה אתכם. אם יש ספק,

© The SANS Institute 2014

פרצו אלי, מה עכשיו?

העבירו את הקובץ להסגר. אם זה לא אפשרי, תמחקו את הקובץ.

- **התקנה מחדש** – אם אתם לא יכולים לנקות את המחשב עם האנטי וירוס, אחת מהדרכים הבטוחות ביותר להתאושש מהמקרה הוא להתקין את המחשב מההתחלה. תחילה נתקו את המחשב מהרשת. לאחר מכן עקבו אחרי הוראות יצרן מערכת ההפעלה. במקרים רבים המשמעות היא להשתמש באפשרות המובנית של התקנה מחדש. אם אפשרות זו אינה עובדת, צרו קשר עם יצרן מערכת ההפעלה על מנת שישלח דיסק התקנה מחדש (Recovery). אל תתקינו את מערכת ההפעלה מהגיבויים. הגיבויים שלכם עלולים להכיל את אותן פגיעויות שאפשרו לתוקף לקבל גישה למחשב שלכם. בגיבויים יש להשתמש אך ורק לצורך שחזור המידע האישי שלכם. בנוסף, אם המחשב שלכם ישן או לא מעודכן זה עשוי להיות פשוט יותר (ואולי אף זול יותר) לקנות מחשב חדש מאשר לנסות לבזבז זמן לבנות אותו מחדש.
- **עזרה מקצועית** – אם אתם חוששים שהותקפתם, אבל מרגישים שאין לכם את הידע כדי לתקן זאת, אולי תרצו למסור את המחשב שלכם לגורם מקצועי. לדוגמא, לאחר שהותקפתם אתם עשויים לגלות שהגיבויים שלכם אינם טובים או לא עדכניים. אתם עשויים להתפתות להעביר קבצים קריטיים כגון תמונות, מסמכים או סרטונים בין המחשב הנגוע שלכם ומחשב חדש. עם זאת, בפעולתכם זו אתם עלולים בטעות להעביר פוגענים ולהדביק את המחשב החדש שלכם באותו זמן. אפשרות בטוחה הרבה יותר היא לקחת את המחשב הנגוע לטכנאי אשר יכול לשחזר לכם את הקבצים בצורה בטוחה מבלי לקחת את הסיכון של להעביר גם את הנוזקה.

למדו עוד

הרשמו ל OUCH! הניוזלטר החודשי למודעות אבטחת מידע, גשו לארכיון OUCH!, בקרו אותנו ב http://www.securingthehuman.org ולמדו עוד על פתרונות מודעות אבטחת מידע של SANS.

מקורות

OUCH! Backups: http://www.securingthehuman.org/ouch/2013#september2013

OUCH! Passwords: http://www.securingthehuman.org/ouch/2013#may2013

OUCH! What Is Malware: http://www.securingthehuman.org/ouch/2014#february2014

Detecting Evil Poster: https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

OUCH! מפורסם ע»י SANS Securing The Human ומופץ תחת רשיון Creative Commons BY-NC-ND ٣,٠. אתם חופשיים להפיץ את הניוזלטר הזה או להשתמש בו בתוכנית העלאת המודעות שלכם כל עוד שאינכם עורכים שינויים בניוזלטר. לתרגום ומידע נוסף אנא צרו קשר ב ouch@securingthehuman.org

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
צוות העורכים: ביל ווייימן, וולט סקריבנס, פיל הופמן, בוב רודיס.