מרכז סליקה בנקאי בע"מ
שירותי בנק אוטומטיים בע"מ
SANS SECURING THE HUMAN
עלון מודעות אבטחת מידע חודשי לכולם

OUCH!

בגיליון זה...

- מה היא הכופרה
- האם כדאי לשלם את הכופר?
- גיבויים
- אמצעי הגנה נוספים

כופרה

מה היא הכופרה?

כופרה היא סוג מיוחד של תוכנה זדונית אשר מתפשטת באופן פעיל ברחבי האינטרנט כיום, מאיימת להשמיד מסמכים וקבצים אחרים של הקורבן. תוכנה זדונית היא תוכנת מחשב המשמשת לביצוע פעולות זדוניות. הכופ־רה היא סוג אחד של תוכנות זדוניות מני רבים, היא הפכה להיות נפוצה מאוד משום שזה רווחי מאוד עבור הפושעים. לאחר שהכופרה מדביקה את המחשב שלך, היא מצפינה קבצים מסוימים או אולי את כל הכונן הקשיח שלך. לאחר ההדבקה אתה יכול להישאר נעול מחוץ למערכת כולה או אינך יכול לגשת לקבצים חשובים שלך, כגון מסמכים או תמונות. לאחר מכן התוכנה הזדונית מודיעה לך כי הדרך היחידה שאתה יכול לפענח את הקבצים שלך ולשחזר את המערכת היא לשלם את הכופר. לרוב הכופר חייב להיות משולם בצורה כלשהי של מטבע דיגיטלי, כגון ביטקוין. הכופרה מתפשטת כמו סוגים אחרים של תוכנות זדוניות. השיטה הנפוצה ביותר היא שליחת מיילים זדוניים לקורבנות. פושעי הסייבר מנסים להטעות אותך ולגרום לך לפתוח קובץ מצורף נגוע או לחיצה על קישור שיוביל אתכם לאתר של התוקף.

עורך אורח
לני זלצר מתמקד בהגנה על מערכות ה- IT של לקוחותיו בחברת NCR, בנוסף הוא מלמד לחימה והתמודדות בתוכנות זדוניות במכון SANS. לני הוא פעיל בטוויטר@lennyzeltser וכותב בלוג האבטחה ב- zeltser.com.

האם אתה צריך לשלם את הכופר?

דילמה קשה. כאשר אנשים משלמים לפושעי הסייבר בעת ההדבקה הפושעים מקבלים יותר מוטיבציה להדביק אחרים. מצד שני, ייתכן כי אין אפשרות אחרת לשחזר את הקבצים. חשוב להדגיש, גם אם אתה משלם את הכופר, אין ערובה שתקבל בחזרה את הקבצים שלך. אתם מתמודדים עם עבריינים, הם יכולים לסרב לפענח את הקבצים, במידה והם מספקים לך את שיטת הפענוח תמורת התשלום, משהו יכול להשתבש במהלך תהליך הפענוח או שהמחשב עלול להיות נגוע בתוכנה זדונית נוספת.

© SANS Institute 2016

גבה את הקבצים שלך

אולי הדרך הטובה ביותר להתאושש מהידבקות בכופרה ולא לשלם כופר היא לשחזר את הקבצים שלך מגיבויים. בדרך זו, גם אם אתה נדבקת בכופרה, יש לך דרך לשחזור את הקבצים לאחר התקנה מחדש של המחשב או לנקות את הכופרה. זכור כי אם הגיבוי מחובר למערכת הנגועה, הכופרה עשויה למחוק או להצפין את קובצי הגיבוי. לכן, חשוב לגבות את הקבצים לשירותים מבוססי ענן מוכרים או לאחסן את הגיבויים על כוננים חיצוניים שאינם מחו־ברים באופן תמידי למערכת שלך. בנוסף, טעות נפוצה שהרבה אנשים עושים עם גיבויים היא להניח שהגיבוי עובד מבלי לבדוק אם הם יכולים לשחזר את הקבצים בפועל. הקפד לבדוק באופן קבוע כי הגיבויים עובדים, ולוודא כי אתה יכול לשחזר את הקבצים שאתה צריך. גיבויים חשובים משום שהם יכולים לסייע בשחזור כאשר אתה בטעות מוחק קבצים או במקרה של קריסת הכונן הקשיח.

הכופרה היא תוכנה זדונית שברגע שהיא מדביקה את המחשב, מצפינה את כל הקבצים במחשב שלך ומונעת ממך גישה אליהם.

אמצעי הגנה נוסף

אתה יכול להגן על עצמך מפני תוכנות כופרה באותו אופן שהיית מגן נגד סוגים אחרים של תוכנות זדוניות, כדי לא להידבק. ראשית, ודא כי יש לך תוכנה אנטי וירוס מעודכנת מספק מהימן. תוכנות כאלו נקראות Anti-Malware, הן נועדו לזהות ולעצור תוכנות זדוניות. עם זאת, אנטי וירוס לא יכול לחסום או להסיר את כל התוכניות הזדוניות. פושעי סייבר מחדשים ומפתחים תוכנות זדוניות חדשות ומתוחכמות יותר שיכולים לחמוק מגילוי. ספקי אנטי וירוס מעדכנים את המוצרים שלהם כל זמן עם יכולות חדשות על מנת לזהות תוכנות זדוניות. במובנים רבים זה הפך להיות מרוץ חימוש, שני הצדדים מנסים להערים אחד על השני. למרבה הצער, הרעים הם בדרך כלל צעד אחד קדימה, ולכן אתה צריך לוודא שאתה מגבה את הקבצים שלך ומיישם את פעולות נוספות בכדי להגן על עצמך, לדוגמא:

- לעתים קרובות פושעי סייבר מדביקים מחשבים או התקנים על ידי ניצול נקודות תורפה בתוכנה. ככל שהתוכנה מעודכנת יותר, פוחתות נקודות התורפה הידועות שיש למערכות שלך ולכן זה קשה עבור פושעי סייבר להדביק אותם. לכן, לוודא שמערכות ההפעלה, יישומים והתקנים מתקינים עדכונים באופן אוטומטי.

כופרה

- מומלץ להשתמש במחשבים בחשבון משתמש רגיל עקב הגבלת הרשאות ולא בחשבונות בעלי הרשאות גבוהות כגון "Administrator" או "Root". זה מספק הגנה נוספת על ידי מניעת סוגים רבים של תוכנות זדוניות מלהיות מסוגלות להתקין את עצמן.
- פושעי סייבר מסוגלים לעתים קרובות לגרום לאנשים להתקין תוכנות זדוניות עבורם. לדוגמא, הם עשויים לשלוח לך הודעת דוא"ל שנראית חוקית, המכילה קובץ מצורף או קישור. אולי הדוא"ל התחזה שהגיע מהבנק שלך או חבר. כדאי להימנע מפתיחה של קובץ מצורף או לחיצה על קישור, זה עלול להפעיל קוד זדוני שמתקין תוכנות זדוניות על המערכת שלך. במידה וההודעה יוצרת תחושה חזקה של דחיפות, זה מבלבל, אם זה נראה טוב מכדי להיות אמיתי, או שיש דקדוק לקוי, זה יכול להיות התקפה. חשוב להיות חשדן, השכל הישר הוא לעתים קרובות ההגנה הטובה ביותר שלך.

הגן על עצמך מפני כופרות ותמשיך לעמוד על המשמר בעת פתיחת קבצים מצורפים לדוא"ל או לחיצה על קישורים, וודא כי עדכנת את תוכנה האנטי-וירוס, הקפד לוודא כי הקבצים שלך מגובים באופן קבוע ותמיד ניתן לשחזר אותן.

למד עוד

הרשם לעלון OUCH! המפורסם אחת לחודש, עלון זה מתמקד במודעות אבטחת המידע, ניתן לקרוא עלונים קודמים וניתן ללמוד על מודעות אבטחת המידע של SANS באתר securingthehuman.sans.org/ouch/archives.

מקורות

דיוג: https://securingthehuman.sans.org/ouch/2014#november2014

מהי תוכנה זדונית: https://securingthehuman.sans.org/ouch/2016#march2016

הצפנה: https://securingthehuman.sans.org/ouch/2016#june2016

גיבויים: https://securingthehuman.sans.org/ouch/2015#august2015

מאמר של מיקרוסופט: https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

קורס SANS FOR610 - הנדסה הפוכה לתוכנות זדוניות: https://sans.org/for610

OUCH! יוצא לאור ומפורסם על ידי חברת SANS Securing The Human, הפצתו ברישיון Creative Commons BY-NC-ND 4.0 license, הנך רשאי להפיץ או להשתמש בעלון זה כעזר לתוכנית מודעות המשתמשים, כל עוד לא בצעת שינויים בעלון זה. לתרגומים או מידע נוסף, אנא פנה ouch@securingthehuman.org.

עורכי המערכת: ביל ויימן, וולט סקריוונס, פיל הופמן, בוב רודיס, שריל קונלי
תורגם על ידי: גדי מרגלית ודרור ענבר

securingthehuman.sans.org/blog /securethehuman @securethehuman securingthehuman.sans.org/gplus