Digital Whisper
Technologic Papers

תקיפת בתי חולים על ידי מטופלים

מאת אמיתי דן (popshark)

הקדמה

לאחר התקיפה על הכור האטומי באיראן ביוני 2010, באמצעות תולעת סטקסנט (Stuxnet), העולם עבר שינוי. ההבנה כי ניתן לבצע פעולות סייבר מתוחכמות הביאה לכך שמדינות החלו לפתח מערכי הגנה ותקיפה קיברנטית, וגם חברות אזרחיות הבינו שיש צורך בהערכות מחודשת לנושא. חשוב להבין איך הצליחו לחדור לתוך המערך האיראני בין היתר מאחר שעלו מספר תיאוריות ביחס לדרך שדרכה הצליחו להחדיר את התולעת. שימוש יעיל במסקנות מאפשר את שיכפול ההצלחה.

בין היתר הועלתה השערה כי באחד מהכנסים שבהם מדעני גרעין אירניים השתתפו, חולקו התקני זיכרון בחינם (Net Stick) וכך, תוך ניצול חולשה אנושית של קבלת מתנות, משתתפי הכנס החדירו את תוכנת התקיפה שהוסוותה בתוך ההתקנים. השערה זו היא הבסיס למחקר שעיסוקו היכן ניתן לתקוף בתי חולים תוך עקיפת מרבית ההגנות הקיימות במעגלי האבטחה החיצוניים.

בתי חולים כמטרת איכות

היכולת לשבש מאגרי מידע של מטופלים לפני ניתוח, לשנות פרטי מטופלים כולל סוגי דם או לפגוע ולשלוט מרחוק במכשירים רפואיים, עלולה להוות מטרת איכות של ארגוני טרור, פשיעה וגופים ואנשים שונים. בעוד שהרווח של ארגוני טרור יהיה פגיעה במורל האוכלוסייה שתפחד לקבל טיפול מבית חולים, ארגוני פשע יכולים לסחוט בצורה זו את בתי החולים כסוג של כופר בתמורה לשחרור מאגר מידע. בו בזמן היכולת לשנות נתונים של פציינט מסוים מאפשרת לגרום לפגיעה בגופו אותו פציינט. לדוגמא, בכיר בממשלה או בחברה עסקית שנסע לקבל טיפול רפואי.

מאחר והיום קיימים רובוטים רפואיים הנשלטים מרחוק ובצורה קולית, חלקם לפרוצדורות רפואיות (דה וינצ'י), ניתן לסמן גם אותם כמטרת איכות. הבעיה שנשארת היא הדרך. בתי חולים רבים מנסים להגן על עצמם ממתקפות קיברנטיות ובניגוד לעבר קיימות הגנות רבות כנגד תוקף חיצוני. אם נחזור לכור האירני, ההשערה בנוגע לשיטת התקיפה הינה מדיה מגנטית לצורך חדירה למערכות הארגון. גם במקרה זה, צריך למצוא את נקודת התורפה הנכונה - שבועת הרופאים.

בניגוד לטיפולים הנערכים בתוך גבולות קופות החולים המנהלת מאגר מידע עצמאי, ישנם טיפולים רפואיים שעל הפציינט להביא אתו את ההיסטוריה הרפואית כדי שיוכל לקבל טיפול הולם. תוצאות של בדיקות רפואיות ניתנות לרוב על גבי מדיה מגנטית. כאשר הפציינט עובר בדיקה בקופת חולים ומגיע לניתוח, הוא מתבקש להביא דיסק עם תוצאות רפואיות רלוונטיות, וזאת נקודת תורפה.

בניגוד לסיפור על טרויה, שבה החדרת הסוס הטרויאני בוצעה בעורמה ובצורת מתנה, כאן בעצם הרופאים פונים בבקשה לכלל המטופלים להביא מדיה מגנטית. זאת הדרך לאפשר טיפול רפואי הולם. מנקודת המבט של התוקף, במקום לתת את ההיסטוריה שלו, הוא תוקף את בית החולים.

בתוך הדיסק שנראה כמו דיסק תוצאות לגיטימי, ניתן להסתיר את כלי התקיפה. וכך, על ידי שימוש במטופלים מתחזים לבצע מתקפות מרובות משתתפים על בתי חולים .תוך זמן קצר ניתן יהיה להחדיר מדיה מגנטית עם כלי תקיפה לכלל בתי החולים במדינה שתותקף.

נקודות תורפה בבתי חולים

לאחר שהבנו את הבסיס והרקע אפשר להתקדם שלב ולהתחיל להתביית על מטרות נוחות להתקפה. מאחר שמערכות רפואיות מנסות לחסוך כסף ומשאבי מערכת עקב זמינות מוגבלת, מטופלים רבים עם שברים או בעיות רפואיות הדורשות צילום פנימי נשלחים לבצע הליך מקדים של בדיקות זולות לפני הבדיקה היקרה יותר.

לרוב המטופל יתחיל בצילום רנטגן רגיל, יעבור ל-CT ורק במידה שאין ברירה, הוא ימתין ויבצע את הבדיקה היקרה בסדרה זו שהנה MRI. לעיתים יש לבצע בדיקה נוספת לאחר תקופה או שבר חוזר. מאחר שבכל שלב התוצאות מתקבלות על ידי מדיה מגנטית, ומכיוון שחובה על הרופאים לראות את ההיסטוריה הרפואית של המטופל ברוב המקרים, הפציינט יכול להביא אתו כל דיסק שיבחר.

אם מחברים את הפאזל לתמונה ברורה, מבינים כי בדיקות רדיולוגיות מהוות דרך יחסית נוחה להכניס מדיה מגנטית תוקפנית לבתי חולים. מאחר שמדובר בעצם בהתקנים לרפואה גרעינית, נסגר כאן מעגל תקיפתי עם מקור השראה לתקיפות עתידיות. תרחיש זה מעלה שאלה נוספת - מהו המכשיר המסוכן ביותר שניתן לפגוע בו?

אחת הדוגמאות היא מטופלים העוברים טיפולים נגד סרטן במכשירי הקרנה. מכשירים אלו הינם בעלי עוצמת הקרנה המיועדת להריגת תאים ביולוגיים. השתלטות על מכשיר מסוג זה לאחר החדרה של מדיה מגנטית, תאפשר את הפיכתו למכשיר שהורג תאים בריאים ובמקרים מסוימים אף ככלי לפציעת אנשים. כלל מכשירי הרדיולוגיה עוברים בדיקות תקופתיות למדידת חריגות קרינה, אך הבדיקות אינן תכופות,

וכפי שכבר למדנו מהמקרה של איראן, ניתן גם לזייף תוצאות של מכשירי ניטור ולמנוע את איתור החריגה.

דוגמה נוספת היא רובוטים רפואיים המבצעים ניתוחים. חדירה למערכת הכריזה של בית חולים בעזרת דיסק מגנטי תאפשר באופן הפשוט ביותר לשלוח הוראות קוליות בזמן ניתוח חודרני לרובוטים המקבלים הנחיה קולית. במקרים מעניינים יותר, ניתן יהיה להשתלט לחלוטין על הרובוט ולפגוע בחיי המטופל.

ברוב בתי החולים בעולם קיימת בקשה מהמטופלים המגיעים למחלקות הרדיולוגיות להביא איתם דיסק עם תוצאות רפואיות. לעיתים גם ניתן להביא תוצאות אלו בהתקן USB. מאחר והשימוש במדיה מגנטית הינו חדש יחסית בעולם הרפואה, ככל שבית החולים מנותק ממחשבים הסיכוי שלו להיות מוגן במקרה זה גדול יותר. לכן, דווקא בתי חולים ומרפאות בעולם המשתמשות בתשלילים מיושנים או נייר להצגת נתונים, מוגנים יותר מפני תקיפות מסוג זה.

לצורך מתקפה מוצלחת תוקף יוכל לבצע הנדסה לאחור של קבצים מסוג DICOM המשמשים את בתי החולים לצורך שמירת נתונים רפואיים, ולדעת היכן להחדיר בהם את קובץ התקיפה תוך חיפוש של Zero Days בקוד התוכנה. מבחינה ויזואלית ופיזית ניתן להעתיק את הקובץ שבדיסק, את הנתונים המודפסים על הדיסק המגנטי ולהטמיע אותם חזרה לתוך הדיסק הנוסף שלתוכו יוחדר אמצעי התקיפה. את הנתונים החזותיים (שם הפציינט, פרטי זהות, ופרטי הבדיקה) התוקף יצרוב בחזית הדיסק השני כך שהדיסק לא יעורר חשד.

איומים נוספים יכולים להגיע מכיוון תיירות רפואית ומסתננים. במקרה של תיירות רפואית, היכולת לשלם למדינה זרה תמורת טיפול מאפשרת לתיירים רפואיים להוות כלי אנושי יעיל במתקפה בווקטור זה, במיוחד מכיוון שלעיתים המטופל מגיע ממדינת אויב. במקביל להם, גם מסתננים הנמצאים במגע עם מבריחי גבול וארגוני טרור עלולים לקבל דיסק תקיפה.

נדרשת היערכות מחדש של בתי החולים

כפי שמאמר זה מציג ניתן כיום להחדיר בקלות אמצעי מדיה מגנטית לצרכי תקיפה בבתי חולים בעולם המערבי. פרצה זו נובעת מהתנהלות אבטחת מידע של בתי חולים בעולם, הכפופה לשבועת הרופאים ומהחובה של הרופאים לרפא, מרכיב אתי הקודם לנהלי מחשוב כאשר ישנה שאלה האם לטפל בחולה או לאבטח מחשב.

בכנס רדיולוגים שבו העברתי הרצאה בנושא נאמר שלא ניתן לצפות מרופא לבצע בדיקה ביטחונית לפציינט. מבחינת פתרונות, צריך לפתח שיטות עבודה חדשות ונדרשת היערכות בכל בתי החולים

ובמערכת הרפואית בכלל בכל הנוגע למטופלים שפוגעים בנהלי בתי החולים ובהתנהלותם. יתכן שאחת המסקנות תהיה שיש לבצע בדיקה ביטחונית לאדם לפני שמאפשרים לו החדרת נתונים רפואיים.

בכל מקרה על בתי החולים והאמונים עליהם להבין כי מתווה האיומים השתנה, ופציינט עוין יכול לפגוע באמצעות מערכות המחשוב בגופם ובשלומם של המאושפזים האחרים.

על המחבר

אמיתי הינו חוקר של סוגיות אבטחת מידע, לוחמת סייבר, פרצות במערכות פיזיות וכשלים בשיטות עבודה. כמו כן, הוא מרצה בנושאי אבטחת מידע בפני פורומים שונים, ונוטל חלק בקבוצת מחקר בנושא סייבר באחת מהאוניברסיטאות בישראל.