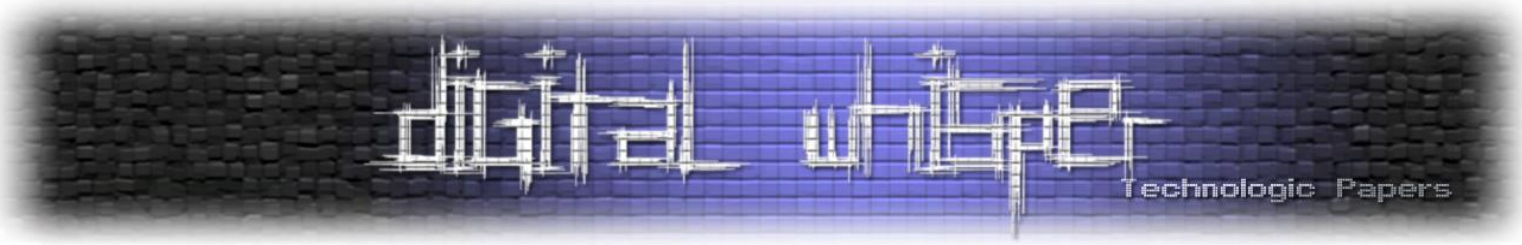


How to turn your KVM into a raging Key-Logging Monster, חלק א' - שסה בי את הבינארי הטוב ביותר שלך!

מאת ליאור אופנהיים ויניב בלמס

הקדמה

סדרת מאמרים זו היא תוצר מחקר שבוצע על ידי הכותבים כחלק מעבודתם בחברת Check Point Software Technologies.

בואו נודה בזה, key-logger-ים הם מגניבים. ממש מגניבים. אפשר למצוא אותם היום בכל פינה, במחשב שלכם, בכבלים שלכם, אפילו במכונת הקפה שלכם. חלקם לגיטימיים (או שלפחות ככה אומרים :), אבל רובם לא. בכל אופן, נראה שהתחום הזה כבר חרוש לגמרי, מה אפשר לחדש כאן? מה כבר אפשר להמציא?

אז זהו, שככה גם אנחנו חשבנו, עד שבוקר בהיר אחד שמנו לב לקופסא ששוכנת לה בנוחות על השולחן, ממש מתחת למסך, וליד כוס הקפה המלוכלכת מאתמול. לקופסא הזאת קוראים KVM. למי שבמקרה לא מכיר, KVM הוא קיצור של Keyboard, Video, Mouse וכל ייעודו בחיים הוא לחבר שני מחשבים (או יותר) לאותו סט של מקלדת, עכבר ומסך. ממש פשוט.

ל-KVM-ים יש היסטוריה מכובדת בעולם המחשבים. בעבר הרחוק, KVM היה פשוט מעגל אלקטרוני שאיפשר לחבר באופן מכני את העכבר המקלדת והמסך לפורט A או לפורט B, תלוי לאיזה מצב סובבת את המתג. (ולכן הוא גם נקרא בלשון העם: 'A/B Switch').

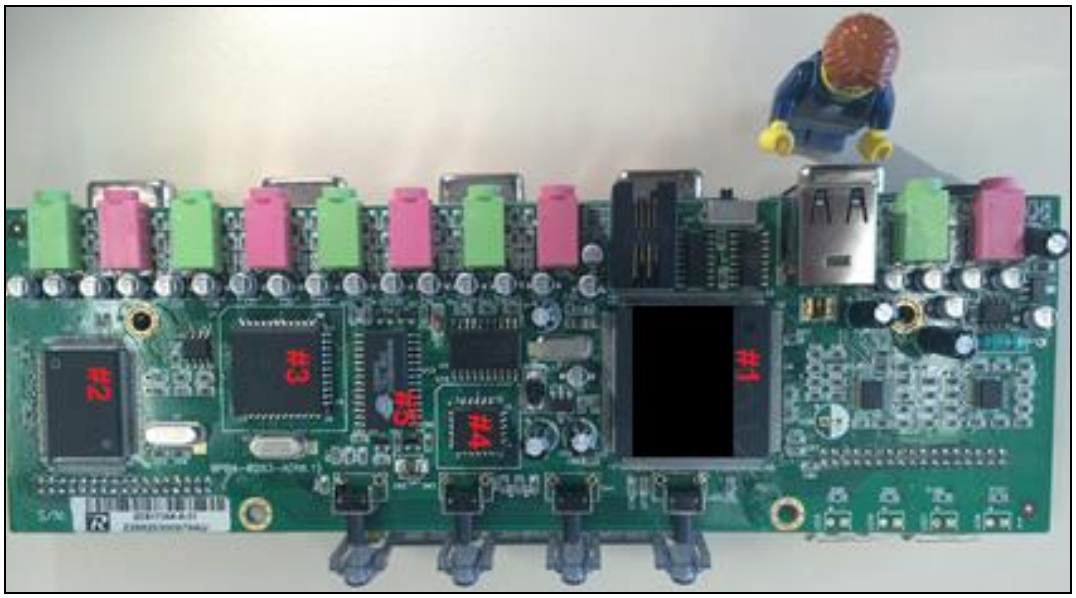
עם השנים ועם התפתחות הטכנולוגיה גם ה-KVMים נעשו הרבה יותר מתוחכמים. היום אפשר למצוא KVMים עם ממשקי קונפיגורציה שמוצגים על מסך המחשב, אפשרות להחליף את הפורטים דרך המקלדת, ואפילו ממשקי web. כמה נוח!

טוב - חשבנו לעצמנו - אז אם KVMים מודרניים הם כאלו מתוחכמים, בטח יש להם מעבד, ואם יש להם מעבד, בטח גם יש להם גם זכרון, ואם יש להם זכרון, בטח אפשר לשתול בו key-logger איכשהו. תחשבו על זה לרגע, key-logger שמותקן על KVM הוא (כמעט) בלתי ניתן לגילוי. אין עקבות על המחשב, כי הקוד

של ה-key-logger לא נמצא עליו, ואין צורך בחיבור שום חומרה חשודה נוספת. המשתמש יכול לאתחל את המחשב, הוא יכול לפרמט אותו, הוא יכול אפילו להחליף אותו במחשב חדש לגמרי, אבל כל עוד ה-KVM שם, כך גם ה-Key-logger שלנו. וכבונוס, בגלל שה-KVM נמצא בצומת של כמה מחשבים, אולי נוכל גם להקליט את ההקלדות של כל המחשבים המחוברים אליו. ואולי, רק אולי, אם נתפלל מספיק חזק לאלוהי ה-KVM, יהיה ניתן להשתמש ב-KVM כערוץ גישור בין שתי רשתות שמבודדות זו מזו ומחוברות בינהן רק דרכו. אבל עוד נגיע לזה בהמשך....

שמחים ומאושרים, עלינו על בגדי עבודה, הכנו אספקה כבדה של אלכוהול והתחלנו לעבוד.

משימה ראשונה - כדי להבין איך לעזאזל להכניס קוד שלנו לתוך ה-KVM, אנחנו צריכים קודם להבין איך בכלל הוא בנוי ואיך הוא פועל. כנראה שיש הרבה דרכים לענות על השאלה הזו, אבל הדרך האהובה עלינו כוללת מברג פיליפס וקצת אלימות.



רושם ראשוני - וואו, מי שם כל כך הרבה אלקטרוניקה בקופסא אחת?! רושם שני - יש האומרים שדברים טובים באים בקופסאות קטנות, אבל במקרה שלנו אולי יהיה יותר נכון לומר - "דברים מעניינים מגיעים בצ'יפים גדולים".

אז כדי להבין מה הולך כאן אולי כדאי להתחיל קודם למפות את הצ'יפים הגדולים שבתמונה, ולנסות להבין מי הם, ומה הם עושים:

- **צ'יפ גדול #1** - גוגל העלה חרס. אין שום מידע פרט לשם היצרן המוטבע על גבי הצ'יפ, אז ככל הנראה מדובר בצ'יפ ייעודי. קופסא שחורה.

- **צ'יפ גדול #2** - אותה תוצאה כמו צ'יפ #1, רק הפעם בצורה של מלבן. עד עכשיו, לא התקדמות מזהירה...
- **צ'יפ גדול #3** - מעבד Winbond 8052. יש! מעולה. למי מכם שלא מכיר, 8052 הוא מעבד מאוד נפוץ בעולם ה-Embedded שמבוסס על ארכיטקטורת intel 8051 (כמו intel 8086, אבל שונה לגמרי). למעבד יש ROM מוטמע בתוכו אשר מכיל את הקוד המורץ (כלומר ה-firmware, להלן "קושחה").
- **צ'יפ גדול #4** - PLD מבית Atmel. גוגל מגלה לנו שPLD הם ראשי תיבות של Programmer Logic Device. סך הכל מדובר ברכיב שניתן לצרוב עליו מעגלים דיגיטליים "לבקשתך", כך שהצ'יפ מבצע לוגיקה מסויימת, שכרגע, אין לנו מושג מהי.
- **צ'יפ גדול #5** - SRAM מבית Lyontek. או במילים אחרות - זיכרון.

למי שבמקרה דילג על הקטע הטכני המתיש לעיל, הנה תקציר - מסתבר שיש מעבד embedded נפוץ בתוך ה-kvm שלנו, ויש לנו הרגשה שהוא בעצם האחראי על הלוגיקה הפנימית של ה-KVM (מין ניחוש מושכל שכזה).

כל שנותר לנו לעשות עכשיו הוא לנסות להשיג את הקושחה של הצ'יפ, לנתח אותה ואז אולי נוכל לטעון למכשיר קושחה חדשה משלנו, ולהתחיל להשתשתע עם המכשיר.

למזלנו, אתר היצרן של ה-KVM שלנו מאפשר הורדת עידכוני קושחה בקלות. טכנית, העדכון עצמו מתבצע דרך כבל סיריאלי המחבר בין המחשב ל- KVM . נחסוך מכם את הניתוח של תוכנת העדכון, ורק נגיד שאחרי כמה מנגנוני הגנה (ובזכות כלי העזר המדהים ל-IDA - DIE) הצלחנו לחלץ מהזיכרון את הקושחה.

במבט חטוף ובעין בלתי מזויינת נראה שהקושחה שחילצנו דחוסה או מוצפנת באופן כלשהו. ערכי האנטרופיה שלה די גבוהים, דבר שתומך בהנחה הזו. גם כל ניסיונות פתיחה שלה ב-IDA (כ-8051 או ככל דבר אחר) עלו בתוהו. אז במקום לצלול לעומק הבינארי ולנסות להבין מה הולך כאן, פשוט לקחנו את הקושחה המחולצת ועם חיוך טיפשי הרצנו אותה ב-binwalk[1] כדי לזהות את סוג הקושחה ו\או מאפיינים בינאריים מעניינים אחרים.

אבל מהר מאוד החיוך הזחוח נמחק מפנינו כשראינו ש-binwalk לא באמת הצליח לזהות את הקושחה, את שיטת הדחיסה, או בעצם כלום, פשוט שום דבר! 0 תוצאות!

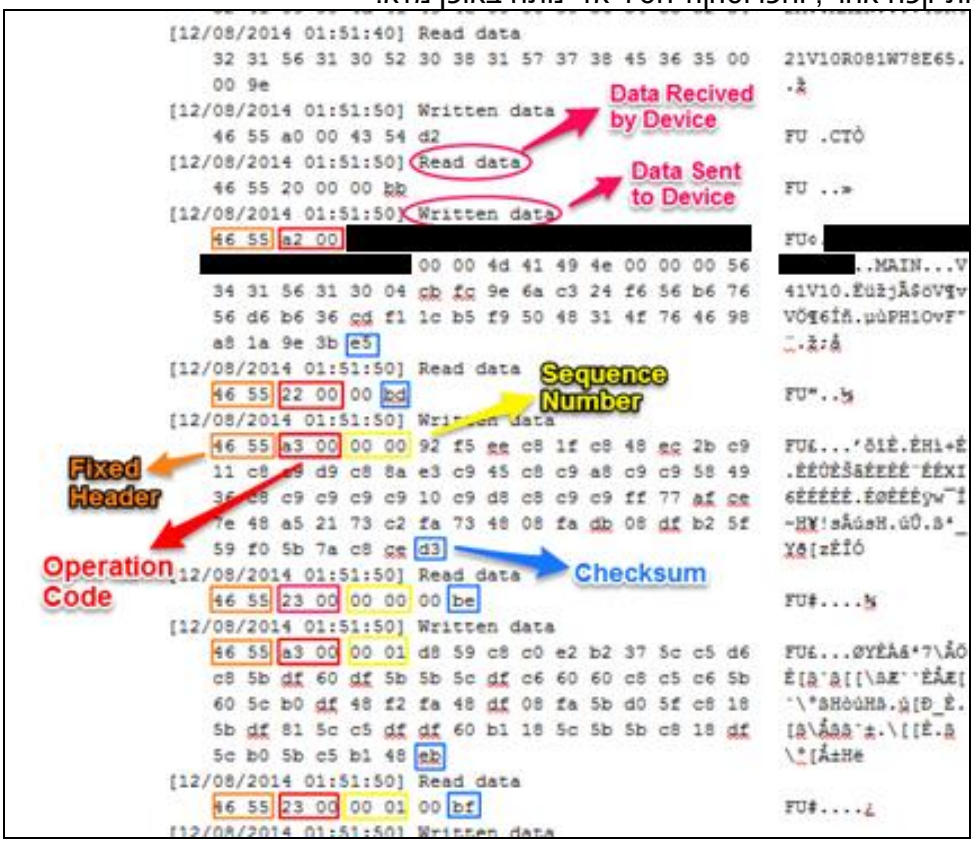
מה עושים?! הנחת העבודה שלנו היא שהקושחה צריכה להפתח מתישהו בתוך תוכנת העדכון, ואז להשלח בצורתה הפתוחה על גבי הכבל הסיראלי הישר אל תוך המכשיר. אם כך, אולי ננסה להיות קצת יותר יצירתיים ובמקום לחקור את תוכנת העידכון, ננסה להסניף את התעבורה שנשלחת ומתקבלת בפורט

[1] Binwalk - כלי נפוץ לזיהוי מגוון רחב של קושחות ידועות, שיטות דחיסה ושאר ירקות.

הסיריאלי. כך בעצם נוכל לחלץ את הקושחה, לאחר שנפתחה ו\או פוענחה, מבלי לדעת את אלגוריתם הדחיסה/הצפנה! נשמע כמו רעיון טוב.

אז הורדנו איזה תוכנה גנרית להסנפה של הפורט הסיריאלי, הרצנו את העידכון והתחלנו להסניף. מהר מאוד ראינו שעל גבי הפורט הסיריאלי מועבר איזשהו פורטוקול, שכפי שאמרנו כנראה מכיל בתוכו את הקושחה המקורית.

כמה כוסות קפה אחרי, והפרוטוקול הסיריאלי נותח באופן מלא:



כמה כוסיות ווסקי אחרי, ויש לנו כלי פייתוני לחילוץ המידע מתוך הפרוטוקול:

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  92 F5 EE C8 1F C8 48 EC 2B C9 11 C8 C9 D9 C8 8A  'õîÈ.ÈHì+É.ÈÉÙÈŠ
00000010  E3 C9 45 C8 C9 A8 C9 C9 58 49 36 C8 C9 C9 C9 C9  ãÉEÈÉ¨ÉÉXI6ÈÉÉÉÉ
00000020  10 C9 D8 C8 C9 C9 FF 77 AF CE 7E 48 A5 21 73 C2  .ÉØÈÉÉÿw¯Î~H¥!sÂ
00000030  FA 73 48 08 FA DB 08 DF B2 5F 59 F0 5B 7A C8 CE  úsH.úÛ.ß²_Yð[zÈÎ
00000040  D8 59 C8 C0 E2 B2 37 5C C5 D6 C8 5B DF 60 DF 5B  ØYÈÀâ²7\ÅÖÈ[ß`ß[
00000050  5B 5C DF C6 60 60 C8 C5 C6 5B 60 5C B0 DF 48 F2  [\ßÆ``ÈÅÆ[`\°ßHò
00000060  FA 48 DF 08 FA 5B D0 5F C8 18 5B DF 81 5C C5 DF  úHß.ú[Ð_È.[ß.\Åß
00000070  DF 60 B1 18 5C 5B 5B C8 18 DF 5C B0 5B C5 B1 48  ß`±.\[[È.ß\°[Å±H
00000080  DF 5B 08 FA 48 F2 FA C8 5B 5C DF 74 18 5F C8 C5  ß[.úHòúÈ[\ßt._ÈÅ
00000090  64 5B 18 5C 60 DF DF 5B 5C C5 B0 5B DF C8 18 64  d[.\`ßß[\Å°[ßÈ.d
000000A0  08 F2 FA 48 5B 48 DF FA DF 5F 27 18 5C F8 5B C8  .òúH[Hßúß_'.\ø[È
000000B0  10 DF 5C 60 5B C5 D0 DF B0 C8 5B DF C5 5B 5C 10  .ß\`[ÅÐß°È[ßÅ[\.
000000C0  FA 48 48 5B F2 D0 08 DF C6 98 60 5C 5F FA DF 5B  úHH[òÐ.ßÆ˜`\_úß[
000000D0  5B C5 D0 FB DF F8 E9 5C C5 B1 F8 5B DF 18 DF FB  [ÅÐûßøé\Å±ø[ß.ßû
000000E0  64 5B 18 5C 08 D0 DF 5B 5B C5 D0 FB DF F8 A8 5C  d[.\.Ðß[[ÅÐûßø¨\
000000F0  C5 D0 F8 5B DF 10 DF FB FF 5B E2 4E C8 D0 77 21  ÅÐø[ß.ßûÿ[âNÈÐw!
00000100  DA 21 63 74 C6 F7 C0 C8 10 E1 5C A5 CE 88 00 F7  Ú!ctÆ÷ÀÈ.á\¥Î^.÷
00000110  73 5F B7 F2 48 21 C2 DB 08 FA FA 48 08 73 DF 27  s_·òH!ÂÛ.úúH.sß'
00000120  DC 21 98 E8 9D AD C8 C6 C0 1E FF D9 3F 40 C8 90  Ü!˜è..ÈÆÀ.ÿÙ?@È.
00000130  21 73 F7 8B 5F 37 FD F9 79 77 5F F7 CC D6 60 77  !s÷‹_7ýùyw_÷ÌÖ`w
00000140  AA DF DF C5 2F C4 DB C0 DB 90 C2 73 37 C8 73 FA  ªßßÅ/ÄÛÀÛ.Âs7Ès ú
00000150  21 48 F7 08 FA 58 5F 27 9D 10 2F DF 60 5C E0 98  !H÷.úX_'../ß`\à˜
00000160  3F C8 1E 40 C6 DC 59 DF 77 7B 21 F1 40 F1 CC FF  ?È.@ÆÜYßw{!ñ@ñÌÿ

                          ■ ■ ■

0000FEB0  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FEC0  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FED0  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FEE0  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FEF0  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FF00  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FF10  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FF20  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FF30  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FF40  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FF50  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FF60  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FF70  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FF80  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FF90  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FFA0  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FFB0  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FFC0  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FFD0  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FFE0  27 27 27 27 27 27 27 27 27 27 27 27 27 27 27 27  ''''''''''''''''
0000FFF0  27 27 27 27 27 27 27 27 6A 4A 51 59 79 27 79 51  ''''''''jJQYy'yQ
```

מצוין! נראה שהקושחה לא דחוסה יותר - ערך האנטרופיה ירד משמעותית. כנראה שאנחנו בכיוון הנכון. חדי האבחנה בינכם גם כנראה ישימו לב לכך שהבית 0x27 חוזר על עצמו בסוף הקובץ. עוד סימן נהדר לכך שהמידע לא דחוס יותר.

אולי עכשיו נוכל לקבל תוצאות טובות יותר מ-binwalk? טוב, אז כנראה זה לא הולך להיות כל כך קל... binwalk ממשיך לסרב בתוקף לזהות את סוג הקושחה או כל דבר אחר, וכנ"ל IDA.

ניסינו לחזור על אותה הבדיקה עם גרסאות עידכון שונות וכצפוי קיבלנו בדיוק את אותן התוצאות. ההבדל הניכר היחידי בין התוצאות היה בבית הריפוד (זה עם הערך 0x27 בתמונה למעלה), ערך הריפוד משתנה בין כל גרסה.

אז למה קיימים ריפודים שונים בגרסאות שונות? הסיבה היחידה שיכולנו לחשוב עליה היא שמדובר בשיטת קידוד פשוטה ומטרתה היחידה היא למנוע מאיתנו לצפות בקוד האמיתי בקלות. ולכן, מכיוון שריפוד באפסים נראה יותר טוב בעין, נשמע לנו מאוד הגיוני לנסות לקסר (פועל: XOR) את כל הקובץ בבית האחרון הזה, וכך לאפס את סוף הקובץ, ובתקוה כך גם שאר הקובץ יהפוך למשהו יותר הגיוני.

אולי הפעם באמת הצלחנו? האם יש לנו עכשיו קוד קריא?

אז זהו, שלא.

אם נסתכל על חצי הכוס הריקה binwalk עדיין לא מחזיר שום תוצאה וגם IDA לא מביאה איזו בשורה מרעננת, אבל אם נסתכל על חצי הכוס המלאה, התגלה לנו משהו די מעניין.

כשמשווים את כל הגרסאות השונות, לאחר פעולת הקיסור, מתגלה דפוס תדירויות מאוד דומה בין הגרסאות. כלומר, אותם הבתים הופיעו מספר דומה של פעמים על פני כל הגרסאות באופן עקבי. זה כנראה אומר שעשינו צעד בכיוון הנכון, כל הגרסאות כתובות עכשיו באותה ה"שפה", כל מה שנשאר לנו להבין הוא איך לתרגם את השפה הזו לקוד בעל משמעות.

למרות שהשגנו התקדמות מסוימת, נותרו המון שאלות פתוחות והפיתרון עדיין לא נראה באופק. כנראה שזה הזמן הנכון לרדת לברזלים[2].

המשך יבוא...

נ.ב.

לאלו מכם שהגיעו עד לחלק הזה במאמר ואינם יכולים להתאפק, הלינק הבא מכיל את גרסת הקושחה במצבה המקורי. אתם מוזמנים לנסות את מזלכם וכישוריכם האישיים ולנסות להפוך אותה לקוד אמיתי (כן, זה לגמרי אפשרי). בהצלחה!

[2] **ברזל** - הוא יסוד כימי שסמלו הכימי Fe ומספרו האטומי 26. הוא גם כינוי נפוץ לשכבה הנמוכה ביותר האפשריתבמערכת כלשהי.