בנטעלם אבטה

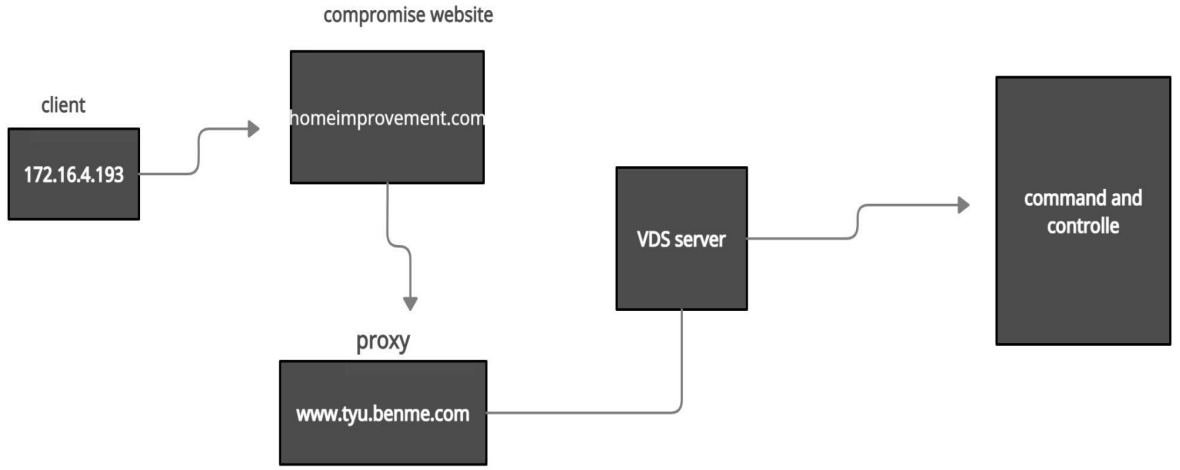
חקירת ransomware ceber exploit kits

Exploit kits

exploit kis הן מגוון רחב של התקפות שונות שהיו נפוצות יותר בשנות 2015-2018 עם הפצות או גרסאות שונות. angler,blackhole,flashpack (הפצת rig שקרתה באירוע שלנו ועלייה נרחיב בהמשך) הן בין ההפצות הנפוצות והמוכרות ביותר.

exploit kit הן שימוש באתרים שנפגעו או שליחת קוד זדוני (malicious malware) למייל אישי של משתמשים על מנת להתקין תוכנה זדונית שתוכל לתת שליטה מלאה לתוקפים שמחזקים בה ושמנהלים אותה על ידי מערכת בקרה ושליטה(cnc) דוגמא:

בגלל החולשות שהיו בדפדפן internet explorer, תוקף מצליח להיכנס לקוד המקור של אתר מסוים ומצליח לשים קישור לאתר עם exploit kit. במקרה הזה המשתמש התמים שלא יודע מה התרחש מאחורי האתר הרגיל , נכנס לאותו אתר פגוע ונשלח לאתר עם הקוד הזדוני שהתוקף שם בקישור.בשלב הזה הקוד הזדוני מחפש תוכנות עם פגיעות כמו adobe flash player ובודק אם יש חולשות על התוכנות האלה במידה ומצא חולשות על תוכנות הללו הקוד מתקים את התוכן שלו (payload) שהוא יכול להיות shell code ,ransomware.



exploit kit rig

הסבר כללי על exploit kit rig- תיקפות משתמשים שגולשים לאתר אינטרנט רגיל על ידי הזרקה קישור מפנה לאתר עם קוד זדוני.בהתקפות מסוג זה התוקף שמנהל את כל האירוע מאחסן קודים זדונים דוגמא סוס טרויאני או ראנסוור שונים בשרת שנקראה server vds המעביר אותם לשרת אינטרנט המשמש לסוג של שרת proxy .שרת זה מחפש חולשות על המחשב הקורבן בתוכנות מבוססות microsoft softwares,adobe flash player ומתקין את הקוד.לאחר התקנת קוד מחשב הקורבן נמצא תחת שליטה של התוקף שיכול לעשות כל מיני מניפולציות שונות דוגמא להצפין את הכל הקבצים של המשתמש ולבקש דמי כופר.

חקירת קובץ ransomware pcap

כפי שניתן לראות מהציור למעלה המשתמש גולש לאתר רגיל homeimprivement.com.

הפקודה tshark -r ransomware -Y "ip.addr ==172.16.4.193" -T fields -e dns.qry.name

מגלה לנו את כל הבקשות dns שהמשתמש עשה ואחת הבקשות היא ל -homeimprovment.com.

התוקף שמנהל את כל האירוע ב command and control ככל הנראה הצליח לשים קישור שמוביל לשרת tyu.benme.com.רוב הזמן בהתקפות מסוג זה התוקפים מנצלים את החולשות שיש בדפדפן ומצליחים לחדור לקוד מקור של אתר מסוים ושמים קישור על ידי תגית html שנקראת iframe.

עם הפקודה "sudo tcpdump -nr ransomware.pcap | grep "iframe אפשר לראות שאכן הייתה יצירה של תגית זו על ידי javascript.

הוכחה נוספת לכך שהמשתמש הועבר מהאתר הרגיל לאתר עם קוד זדוני היא התראה שקיבלנו בטוטאל וירוס. אחת התראות שם מספרת לנו שהייתה התנהגות לא רצויה ב www.tyu.benme.com. לאחר שעשינו את הפקודה הבאה

Tshark -r ransomware.pcap -Y “http.host == tyu.benme.com” -T fields -e http.referer

אפשר לראות שאכן האתר הרגיל הוא זה שהפנה את המשתמש לאתר עם הקוד הזדוני.

אתר tyu.benme.com הוא זה שהתקין את ransomware ceber על מחשב המשתמש. התוכנה שדרכה הצליח להתקין את הקוד היא תוכנה של adobe flash player שהמשתמש התקן על המחשב האישי שלו ההוכחה לכך היא הפקודה הבאה:

Tshark -r ransomware.pcap -Y “http.host == fdpdownload2.macromedia.com”

פקודה זו היא אינדיקציה לכך שהמשתמש התקין תוכנה עם חולשה כלשהי שהתוקף הצליח לנצל אותה

ההוכחה שהקוד הותקן על מחשב המשתמש היא הפקודה הבאה:

Tshark -r ransomware.pcap -Y “http.host == tyu.benme.com and http.request.method ==POST” -T fields -e http.referer

פקודה זו מראה לנו שהייתה שליחת מידע לשרת מרוחק לא דרך דפדפן . השליחה הזו התבצעה ככל הנראה על ידי הקוד הזדוני שיושב בתוך המחשב של המשתמש על ידי תוכנה כלשהי שהיא לא דפדפן.

בהתבסס על מערכות של המשתמש שהן ווינדוס ומערכת לניגון סרטים שדרכה הותקן הקוד סביר להניח שהפורמט של הקוד הזדוני יהיה קובץ הרצה מסוג exe.

עם הפקודה הבאה אפשר לראות את כל השיחה שהייתה בין המשתמש לשרת התוקף.

Tshark -r ransomware.pcap -Y “ip.addr ==194.87.234.129”

לפי הפקטות בשיחה הזו אפשר לראות ולהבין שאכן הייתה התקנה של קובץ מסוים.קובץ עבר ברשת כמובן בחלקים קטנים

```
eliot@eliot-VirtualBox: ~                                   eliot@eliot-VirtualBox: ~
eliot@eliot-VirtualBox: ~ 173x61
5767 189.376845 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=112563 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5768 189.377015 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=113884 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5769 189.377125 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=115205 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5770 189.377200 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=115205 Win=64729 Len=0
5771 189.377239 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=116526 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5772 189.377448 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=117847 Win=64729 Len=0
5773 189.392575 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=117847 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5774 189.392776 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=119168 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5775 189.393024 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=120489 Win=64729 Len=0
5776 189.408090 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=120489 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5777 189.408242 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=121810 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5778 189.408369 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=123131 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5779 189.408459 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=123131 Win=64729 Len=0
5780 189.409707 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=124452 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5781 189.409909 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=125773 Win=64729 Len=0
5782 189.423834 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=125773 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5783 189.424021 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=127094 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5784 189.424254 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=128415 Win=64729 Len=0
5785 189.439334 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=128415 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5786 189.439487 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=129736 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5787 189.439614 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=131057 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5788 189.439729 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=132378 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5789 189.439757 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=131057 Win=64729 Len=0
5790 189.439999 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=133699 Win=64729 Len=0
5791 189.455079 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=133699 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5792 189.455330 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=135020 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5793 189.455530 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=136341 Win=64729 Len=0
5794 189.547076 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=136341 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5795 189.547262 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=137662 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5796 189.547372 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=138983 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5797 189.547519 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=140304 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5798 189.547534 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=138983 Win=64729 Len=0
5800 189.547779 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=141625 Win=64729 Len=0
5810 189.548706 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=141625 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5814 189.549014 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=142946 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5815 189.549245 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=144267 Win=64729 Len=0
5832 189.575117 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=144267 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5833 189.575152 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=145588 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5834 189.575244 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=146909 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5835 189.575504 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [PSH, ACK] Seq=148230 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5836 189.575506 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=146909 Win=64729 Len=0
5837 189.575757 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=149551 Win=64729 Len=0
5838 189.595826 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=149551 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5839 189.595862 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=150872 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5840 189.596147 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=152193 Win=64729 Len=0
5841 189.659848 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=152193 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5842 189.660050 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=153514 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5843 189.660178 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=154835 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5844 189.660282 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=154835 Win=64729 Len=0
5845 189.660292 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=156156 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5846 189.660528 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=157477 Win=64729 Len=0
5853 189.674060 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=157477 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5854 189.674096 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=158798 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5855 189.674400 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=160119 Win=64729 Len=0
5856 189.689320 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=160119 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5857 189.689541 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=161440 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
5858 189.689808 172.16.4.193 ? 194.87.234.129 TCP 60 49223 ? 80 [ACK] Seq=480 Ack=162761 Win=64729 Len=0
5873 189.762117 194.87.234.129 ? 172.16.4.193 TCP 1375 80 ? 49223 [ACK] Seq=162761 Ack=480 Win=30016 Len=1321 [TCP segment of a reassembled PDU]
```

כפי שניתן לראות למעלה אכן הייתה תהליך של התקנת קובץ מסוג exe בהתבסס על מערכות שיש על המחשב של המשתמש לכן נעשה את הפקודה הבאה על מנת לראות איפה הקובץ הזה נמצא וננסה לרכז מידע.

Tshark -r ransomware.pcap -T fields -e tcp.stream -e frame.number -e data | grep "4d5a"

פקודה זו נותנת לנו את מספר שיחה ומספר פקטה שהייה בהם תהליך הקשור לקובץ מסוג exe

ceber ransomware

תוכנה זדונית מטרתה לגנוב להצפין מידע.לאחר קוד זדוני מסוים הצליח לחדור לתוך רשת ארגונית או לתוך מחשב אישי של לקוח מתחיל תהליך של התקנת תוכנה זדונית.תוכנות זדונית יכולות להיות תכנה שפותחות

שירותים(services) על מנת לפתוח זרימת שיחה בין מחשב הנתקף למחשב התוקף לטובת הדלפת מידע אישי וקריטי או לטובת הצפנת המידע של הנתקף על מנת לדרוש דמי כופר.ceber ransomware הוא מסוג תוכנות שמצפינות את המידע כדי לדרוש תשלום מסוים.

לאחר התקנה התוכנה, המשתמש מקבל ההודעה שהמידע שלו מוצפן כדי לפענח את ההצפנה עליו לשלם תשלום מסוים. בדרך כלל התוכנות המשמשות בשביל להציג את ההודעה הן תוכנות שהקוד הזדונית הצליח לחדור דרכן. למשל במקרה שלנו התוכנה הותקנה דרך התוכנה של adobe flash player ולכן סביר להניח שההודעה תוצג כך