דוח מעבדה עבור הנוזקה MIRAI BOTNET

מגיש יגאל נאמן

שם הוירוס Mirai Botnet

<u>טרם התחלנו..חשוב לציין , שאת הבוטנט עצמו מקמפלים אך ורק בסביבת Kali linux</u>

<u>(קיים סקריפט ייעודי לכך שמאפשר ליצור את האקספלוייט עם כל הכלים האפשרים , כגון: בחירת השרת שיתחברו הבוטים שלכם, לאיזה פורט וכו ...' הסקריפט (התולעת\וירוס)עצמו נכתב בפייתון.'</u>

סוג MIRAI BOTNET IOT

שמות mirai.sys mirai.py mirai.js mir.awx mirai.agobot.gez mirai.dll mirai.conf

שיטות עבודה: הוירוס מופץ בעזרת ניטור הרשת 'SWAP

היא סורקת ברשת האירגונית וגם יוצאת החוצה SCAN RANGES CALSS of iot

האם הישתמשו בחולשה? כמובן. הנוזקה סורקת ברשת האינטרנט כתובות IP

עם רשימות של שם משתמש וסיסמה דיפולטיביות (BY DEFAULT)

של מוצרים חשמליים כגון: ראוטרים, מצלמות, וכיוצא בזה...

שיטות הפצה: כמו שציינתי לעיל, הוירוס עצמו מפיץ עצמו בפעמים הראשונות דרך שרת ה C&C COMMAND CONTROL של התוקפים.

הבוט הראשון, רץ בעזרת המחשב התוקף, התוקף מריץ את הנוזקה ממערכת VMWARE

כל שהיא בשביל לא להדביק את עצמו בתולעת, ולאחר מכן הוא מבצע סריקה מהמחשב לכתובת אייפי מסויימים לאחר שהוירוס מוצא חולשות בכתובות מסויימות הוא מבצע את הפקודה

PSEXEC n

מה שזה בעצם עושה זה מריץ את התולעת במחשב התוקף לאחר שזוהתה החולשה.

התולעת מעתיקה את עצמה ל-

%usr%/%etc%בלינוקס

חשוב לציין שזוהי תולעת שמבוססת LINUX \ ANDROID

זאת אומרת שזאת תולעת שמחפשת חולשות במכשירים שיש עליהם מערכות הפעלה מסוג LINUX

אשר לא מעודכנות כראוי, ולשם היא עושה UPDATE

דבר נוסף הוא שצריך לדעת ולקחת במחשבון זה שהוירוס התולעת עצמה בעצם יש לה חידושים ושיכלולים היא יודעת לסרוק טבלאות SQLג

ולבצע את הסריקה והפריצה עצמה מבלי לעלות חשש בטבלאות כיוון שהיא משתמשת ב- ATTRIBUTES

זאת אומרת היא יודעת להסתיר את הקבצים שהיא מעלה לאחר שהיא מבצעת PSEXEC

לקבצי הנוזקה.

ביצוע ATTRIBUTEלקבצים בפקודת ה- SHELL

תגרום לכך שמנהל הרשת SYSTEM ROOT ADMINISTRATOR

לא יוכל לראות את הקבצים (גם אם הוא יגדיר במחשב להציג קבצים מוסתרים הוא עדיין לא יראה אותם)

והדרך היחידה יהיה לראות את הקבצים זה אך ורק דרך פקודת ה- SHELL

ע"י ביצוע הפקודה ב terminal

ATTRIB +H +S +N FILE

המשך לכתבה שפורסמה בהקשר ל ;MIRAI BOTNET

פרצת אבטחה חמורה התגלתה בראוטרים שלNetgear

ש לכם ראוטר של ?Netgear זה הזמן לבדוק את הגדרות המכשיר ולעדכן תוכנה; פרצה חדשה שהתגלתה מאפשרת לתוקפים לקבל מרחוק גישה מלאה על הראוטר שלכם ולהפוך אותו לבוט-נט

לפני כשלושה חודשים **הפילה מתקפת DDoS** את ספקית ה DNS-האמריקאית חברת ;Dyn

כתוצאה מכך כמה מאתרים הגדולים בעולם ביניהם אמזון, טוויטר, ספוטיפיי Shopify, וסאונדקלאוד

לא היו זמינים למשך שעות ארוכות. האצבע המאשימה הופנתה כלפי מכשירי IoT שונים כמו

ראוטרים ומצלמות אבטחה עם רמת אבטחה נמוכה, בהם נעשה שימוש לצורך המתקפה. עתה,

טוענת חברת **Trustwave** כי גילתה פרצת אבטחה בראוטרים של היצרנית הפופולארית ,Netgear

שמאפשרים לכל האקר להפוך את הראוטר שלכם לבוטנט.

מיליון ראוטרים ברחבי העולם חשופים לפרצה

הדוח של Trustwave חושף פרצת אבטחה שקיימת ב-31 דגמים שונים של ראוטרים של

Netgear(נטגיר) ויותר ממיליון מכשירים שונים ברחבי העולם. הפרצה מאפשרת לתוקפים לעקוף

את מערכת הכניסה לממשק הניהול של הראוטר שלכם ולמעשה לקבל זכויות אדמין – התולעת

משתמשת בסיסמאות דיפולטיביות של הראוטר.

הפרצה מאפשרת לכל תוקף לשלוח request לקובץ ה passwordrecovered.cgi-בראוטר,

ובתגובה לקבל את שם המשתמש והסיסמה כטקסט פשוט ולא מוצפן .Cleartext –

עם זאת, האפשרות זמינה רק עבור משתמשים שבחרו להפעיל את האפשרות של השליטה

מרחוק על הראוטר שלהם.

בבדיקה ראשונית שעשה סיימון קנין, החוקר שגילה את הפרצה,

הוא מצא יותר מעשרת אלפים ראוטרים שמחוברים כרגע לרשת וחשופים לפרצה,

עם זאת, הוא התריע כי מאות אלפי ראוטרים אחרים מחוברים לרשתות פנימיות וחשופים גם הם

למתקפה על ידי גישה לוקאלית.

כך למשל יכול תוקף לשנות את הגישה ברשתות WiFi ציבוריות כמו בתי קפה או ספריות.

הבאג התגלה למעשה כבר בחורף של 2016, כאשר קנין חווה בעיות בראוטר.

מכיוון שהיה זה חורף קר והוא היה כבר במיטה החמה, הוא התעצל לדבריו לרדת לעשות ריסטארט למכשיר.

במקום זאת, הוא ניסה לבצע ריסטארט מממשק השליטה מרחוק, וכאשר גילה שהוא לא זוכר את הסיסמה, הוא ניסה, כמו כל חוקר אבטחה טוב, לשחק קצת עם הממשק, עד אשר גילה את הפרצה, שהתבססה על **פרצות** **ותיקות** יותר.

קנין התריע בפני Netgear כבר באפריל 2016, אולם רק עכשיו, לאחר שהחברה סיימה את העבודה על עדכוני האבטחה, הוא מפרסם את קיום הפרצה.

עם זאת, מתוך 31 הדגמים, החברה שחררה עדכון קושחה (Firmware) ל-20 דגמים בלבד .

Netgearמסרה בתגובה: "הפרצה הזו תלויה בכך שהתוקף יכול להשיג גישה לרשת פנימית או כאשר אפשרות ה'ניהול מרחוק' הופעלה בראוטר.

האפשרות הזו כבויה כברירת מחדל ומשתמשים יכולים לכבות אותה בכל רגע על ידי כניסה ל'הגדרות מתקדמות.'"

ההמלצה המיידית היא כמובן לכבות את האפשרות של שליטה מרחוק על הראוטר ובמקביל **לעדכן** **את ה Firmware-בדף הייעודי** שפתחה החברה.

שם תוכלו גם לקבל את רשימת הדגמים המלאה, בהם התגלתה הפרצה.

עוד?

חודש וחצי לאחר מכן דיווח נוסף על חידוש התועלת.

האתר של בריאן קרבס, חוקר האבטחה האמריקאי, שחשף לא מעט האקרים ושיטות פעולה סבל ביומיים האחרונים מאחת ממתקפות ה DDoS-החמורות ביותר מעולם. החידוש: התוקפים השתמשו בתקיפה במכשירי IoT דוגמת מצלמות. החוקר רומז שהאחראיים לכאורה על המתקפה הם צמד נערים ישראלים

אחת מהמתקפות החמורות ביותר בתולדות האינטרנט'

בפוסט שהעלה קרבס הוא חשף כי במשך יומיים בשבוע שעבר, ספג האתר מתקפת DDoS, או מתקפת מניעת שירות מבוזרת, בהיקף עצום של 665 .Gbpsלדברי חברת Akamai, שאחראית על ההגנה על האתר, מדובר במתקפה הנרחבת ביותר בה נתקלה החברה, כשהמתקפה הנרחבת ביותר עד זו היתה בהיקף של 363' Gbpsבלבד'. למעשה, המתקפה היתה כל-כך חריגה בעוצמתה שהיא גרמה ל Akamai,-לא סטארטאפ צעיר, אלא חברת ענק ששוה יותר מ-2.5 מיליארד דולר, לנטוש את קרבס ולשלוח אותו להיות אדון לגורלו.

אולם חוץ מההיקף חסר התקדים, הרי שהמתקפה החדשה הביאה איתה עוד 'בשורה'. מסתבר שמי שתקף את האתר לא היתה בוט-נט רגילה, כלומר רשת מחשבים שנדבקו בנוזקות, ופועלים על ידי פקודה מרחוק, אלא בוט-נט שמתבסס על מכשירי IoT דוגמת מצלמות אבטחה.

המטרה: יותר מ-200 מיליארד מכשירי IoT

כאמור, המתקפה התבצעה על ידי נוזקה בשם Mirai, שמכוונת להדביק מכשירי IoT.

מרגע שהמכשיר נדבק, פועלת הנוזקה ברקע ומחכה לפקודת הפעלה **מרחוק**.

ברגע שזו מגיעה, פועלת הנוזקה תוך כדי התחזות לפקטות

GRE או generic routing encapsulation, פרוטוקול לתקשורת בין מכשירים שונים ברשת.

הנוזקה מקבילה ל Mirai-היא ה Bashlight, שגם היא מיועדת למכשירי IoT.

על פי חברת Level3 Communications, אחראית Bashlight לבוט-נט של יותר מ**מיליון מכשירים.**

נכון, מיליון נשמע מספר מרשים ומרתיע. אבל על פי **התחזיות של אינטל** תוך 4 שנים יגיע מספר מכשירי ה IoT-השונים ל-200 מיליארד.

עכשיו, נותר לנו רק לדמיין את פוטנציאל ההרס של מתקפות שמתבסוסות על יותר ממיליארד מכשירי IoT.

החוקר 'רומז' על קשר לנערים הישראליים

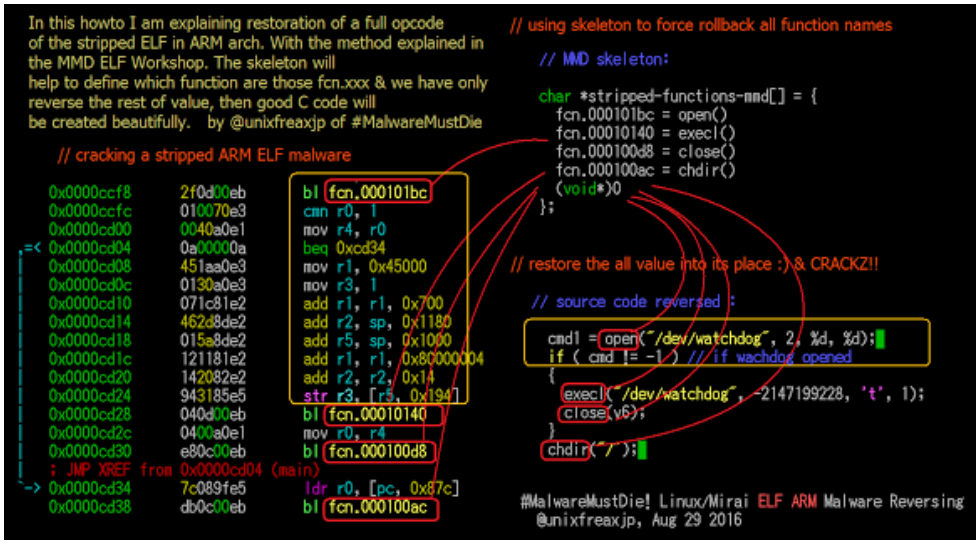
לפני כחודש חשף בריאן קרבס את פעילותו של אתר vDOS, שהציע מתקפות DDoS. קרבס, שהצליח להניח את ידיו על מאגרי מידע של האתר שבאופן אירוני נפרץ, טען אז כי מי שעומדים מאחורי האתר הם איתי חורי וירדן בידני, שני צעירים ישראליים בני 18.

חורי ובידני, שנעצרו מאוחר יותר על ידי המשטרה, הכחישו כל מעורבות באתר.

אבל האם אכן יש קשר בין המקרים? קרבס אמר שאינו בטוח, אבל לדעתו קיים קשר.

לדברי החוקר, בחלק מהשאילתות הופיעה המחרוזת 'freeapplej4ck', הכינוי של אחד מצמד מפעילי האתר.

קובץ באסמבלר איך נראה הוירוס



כך נראה התמונה של חלק מ ה- LOGINשהתולעת מנסה לפצח בעזרת מילון מובנה