Technologic Papers

בוטנט במעגל-סגור

מאת עופר גייר, אור וילדר ויגאל זייפמן

הקדמה

כמו כולכם, גם לנו יצא לקרוא לא מעט אודות האיומים העומדים מאחורי המושג "Internet of Things". מליוני רכיבים בעלי הגנה מועטת מחוברים לאינטרנט ורק מחכים להפרץ ע"י האקרים-מזדמנים שיעשו בהם כרצונם.

עולם ה-IoT הינו נושא המתפתח בתקופה זו, ובדיוק מסיבה זו, גם עולם הנוזקות הקשורות לקטגוריה זו מתפתח. בעקבות תחום העיסוק שלנו, יצא לנו להתקל לא פעם בנוזקות שונות ומשונות, וסביר היה להניח שנתקל בנוזקות הקשורות לעולם זה (ואף לדווח עליהן).

המאמר הבא מגולל את סיפורה של גרסא חדשה של נוזקה חדשה-ישנה שיצא לנו לחקור. הזהרנו עליה לראשונה במרץ 2014, כאשר ראינו גידול של 240 אחוזים בפעילות הבוטנטים בעזרת הכלים איתם אנו מנטרים את הרשת.

מבדיקה שעשינו נראה היה כי רוב הפעילות הגיעה ממצלמות CCTV פרוצות. עובדה זו לא מפתיעה, בהתחשב בכך שמצלמות טלוויזיה במעגל סגור הן בין מכשירי IoT הנפוצים ביותר כיום באינטרנט. דיווחים מראים כי בשנת 2014, היו למעלה מ-245,000,000 מצלמות מעקב הפועלות ברחבי העולם, ואלו רק המצלמות המותקנות באופן מקצועי. ישנן מיליוני מצלמות נוספות שהותקנו על ידי אנשי מקצוע לא מוסמכים.

מספרים אלה, וחוסר מודעות אבטחה מקוונת מצד בעלי מצלמה רבים, הן הסיבות מדוע בוטנטים במצלמות אלו הם חלק מהאויבים הוותיקים ביותר שלנו. ובכל זאת, לאויבים ישנים ישנה היכולת להפתיע, כפי שקיבלנו תזכורת לאחרונה, כאשר אחד הלקוחות שלנו הותקף על ידי התקפות חוזרות ונשנות של HTTP Get Flood.

בשיא, ההתקפה הגיעה ל-20,000 בקשות לשנייה (RPS). אך ההפתעה הגדולה הגיעה מאוחר יותר, כאשר בבדיקת כתובות ה-IP של התוקפים גילינו שחלק מחברי הבוטנט היו ממוקמים ממש בחצר האחורית של משרדי החברה שלנו.

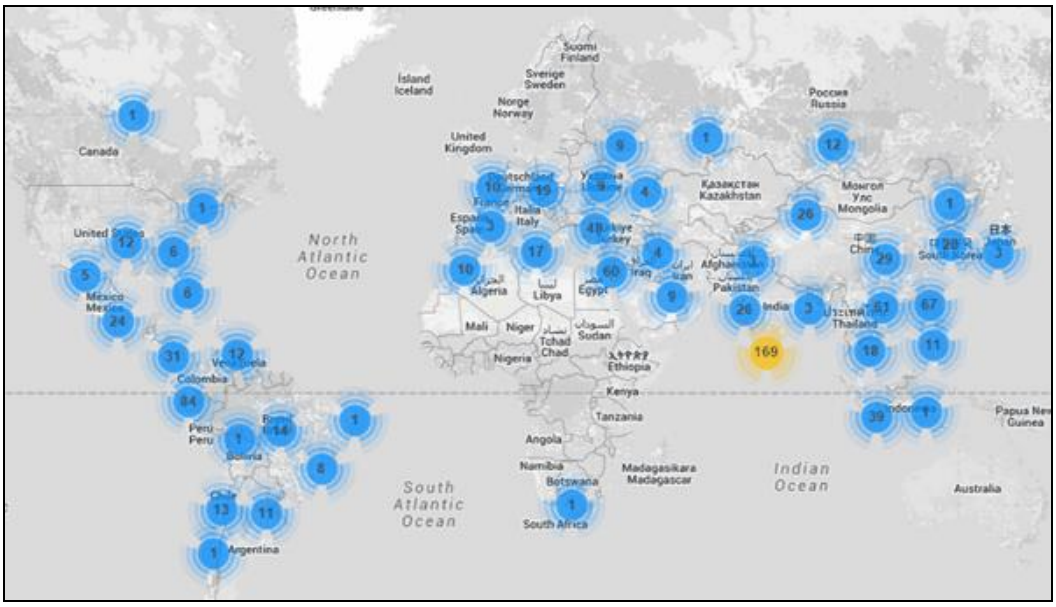
החקירה של כתובות ה-IP התוקפות הראתה שהן שייכות למצלמות טלוויזיה במעגל סגור, כולן נגישות באמצעות סיסמאות ברירת המחדל שלהן. אך זה לא הכל - במבט דרך עדשת המצלמה גם הבחנו בחנות מוכרת בקניון הממוקם לא פחות מחמש דקות נסיעה מהמשרדים שלנו!

ראינו זאת כהזדמנות לתת שירות טוב לקהילה, ולכן קפצנו במכוניות שלנו ונסענו לטיול בקניון ☺. הצלחנו להיפגש עם בעלי החנות, להראות להם איך המצלמות שלהם נוצלו על מנת לתקוף את לקוחותינו ועזרנו להם לנקות את התוכנות הזדוניות מהכונן הקשיח של המצלמה הנגועה.

בזמן שעשינו זאת ראינו את המצלמה שולחת בקשות תקיפה עד הרגע האחרון...

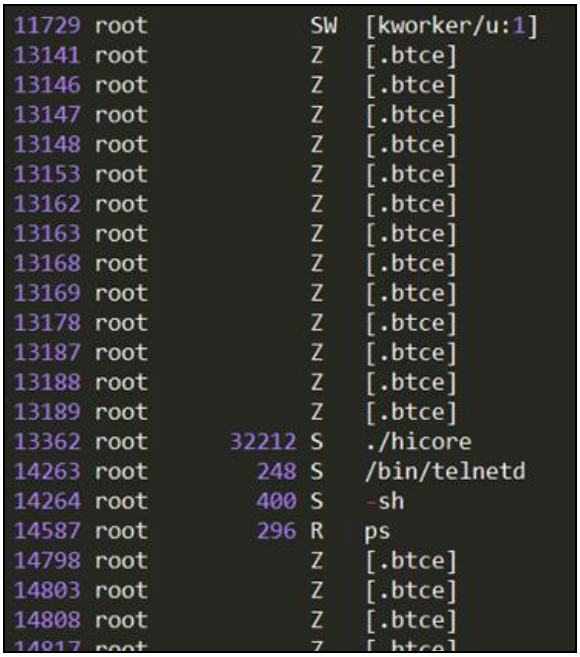
פרטי המתקפה

כאמור, תקיפה זו כללה הצפות של חבילות HTTP GET שנעו לשיא של 20,000 RPS. ממחקר שביצענו, ראינו כי מקור הרעש מגיע מכ-900 כתובות IP של מצלמות CCTV המפוזרות מסביב לעולם. היעדים שלהם היו נכס יחסית נדיר בשימוש של ספקית שירות ענן גדולה.



כלל הרכיבים שהשתתפו במתקפה, הריצו Embedded Linux עם BusyBox - חבילת כלי Unix נפוצים אשר אוגדו תחת בינארי אחד שעוצב (בדרך כלל) עבור מערכות מועטות משאבים.

הקוד הזדוני שמצאנו בהם היה קובץ ELF, שקומפל ל-ARM, שמו היה btce., והוא היה גרסא של ELF_BASHLITE (מוכר גם כ-Lightaidra ו-GayFgt). קוד זדוני שתפקידו לסרוק רכיבי אינטרנט שמריצים BusyBox ומאזינים ל-Telnet או SSH ופגיעים למתקפת BruteForce מבוססת מילון.



במקרה שלנו, הגרסא הזו הגיעה עם יכולת נוספת - לבצע תקיפות HTTP Get Flood מתוך הרכיב שהנוזקה השתלטה עליו. הרצנו על הבינארי strings וקיבלנו (מלבד הסיסמאות שאותן הוא מנסה לנחש) מספר לא קטן של מחרוזות המשמשות אותו בתור User-Agent. לדוגמא:

- Mozilla/4.0 (compatible; MSIE 6.0; MSIE 5.5; Windows NT 5.0)
- Opera 7.02 Bork-edition [en] Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
- Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
- Mozilla/4.0 (compatible; MSIE 8 .0; Windows NT 6.0; Trident/4.0;)
- Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2)
- Gecko/20100115 Firefox/3.6 Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:13.0)
- Gecko/20100101 Firefox/13.0.1 Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:13.0)
- Gecko/20100101 Firefox/13.0.1
- Opera/9.80 (Windows NT 5.1; U; en)
- Presto/2.10.229 Version/11.60

במהלך המחקר שלנו, בדקנו מאילו כתובות IP התחברו למצלמות האבטחה שניטרנו. נראה היה כי התחברו אליהן ממספר רב של כתובות שונות. סימן לכך שהן ככל הנראה נפרצו על-ידי מספר האקרים שונים. עובדה המראה עד כמה קל לאתר ולפרוץ לאותן רכיבים.

דוגמא ל-Netstat שהבאנו מאחת המצלמות:

```
0 ::ffff:10.0.0.21:telnet        ::ffff:60.x.x.57:41238     ESTABLISHED
0 ::ffff:10.0.0.21:telnet        ::ffff:85.x.x.175:42836    ESTABLISHED
0 ::ffff:10.0.0.21:telnet        ::ffff:31.x.x.114:21833    ESTABLISHED
0 ::ffff:10.0.0.21:telnet        ::ffff:14.x.x.49:4344      ESTABLISHED
0 ::ffff:10.0.0.21:telnet        ::ffff:36.x.x.70:33348     ESTABLISHED
0 ::ffff:10.0.0.21:telnet        ::ffff:222.x.x.237:49593   ESTABLISHED
0 ::ffff:10.0.0.21:telnet        ::ffff:201.x.x.157:42611   ESTABLISHED
0 ::ffff:10.0.0.21:telnet        ::ffff:60.x.x.90:51354     ESTABLISHED
0 ::ffff:10.0.0.21:telnet        ::ffff:88.x.x.139:42413    ESTABLISHED
0 ::ffff:10.0.0.21:telnet        ::ffff:219.x.x.139:55355   ESTABLISHED
0 ::ffff:10.0.0.21:telnet        ::ffff:49.x.x.29:44295     ESTABLISHED
0 ::ffff:10.0.0.21:telnet        ::ffff:60.x.x.111:50127    ESTABLISHED
```

[ניתן לראות כמה כתובות IP שונות מחוברות ברגע נתון]

קצת על ה-Malware עצמו

כאמור, הנוזקה עצמה הינה גרסא משודרגת של BASHLITE. שרת ה-C&C נקבע Hardcoded בעת הקמפול. הפקודות שהיא תומכת בהן הן:

- PING
- GETLOCALIP
- SCANNER
- HOLD
- JUNK
- KILLATTK

- **PING** - בעת שליחת הפקודה **PING** הבוט מחזיר את התשובה "**PONG!**" - כך השרת יכול לדעת שהבוט עדיין שם, ובעצם לשלוט ברשת ה-BotNet שלו ולדעת כמה מהם אונליין בכל רגע נתון.
- **GETLOCALIP** - הפקודה **GETLOCALIP** תגרום לבוט להחזיר את התשובה:

```
My IP: [LOCAL_IP]
```

- **SCANNER** - הפקודה **SCANNER** הינה דגל שמצבו הינו "ON" או "OFF", הפקודה מורה לבוט להתחיל או להפסיק לסרוק אחר עוד מערכות פגיעות ולנסות להדביק אותן.

אופן ההדבקה מתבצע ע"י סריקת טווחי IP עבור כתובות המאזינות בפורט 23 (הפורט הדיפולטיבי של Telnet). במידה ואכן נמצאה כתובת כזו, מתבצע ניסיון להתחבר לאותו הפורט בעזרת שמות המשתמשים:

```
root
toor
admin
user
```

ובעזרת הסיסמאות:

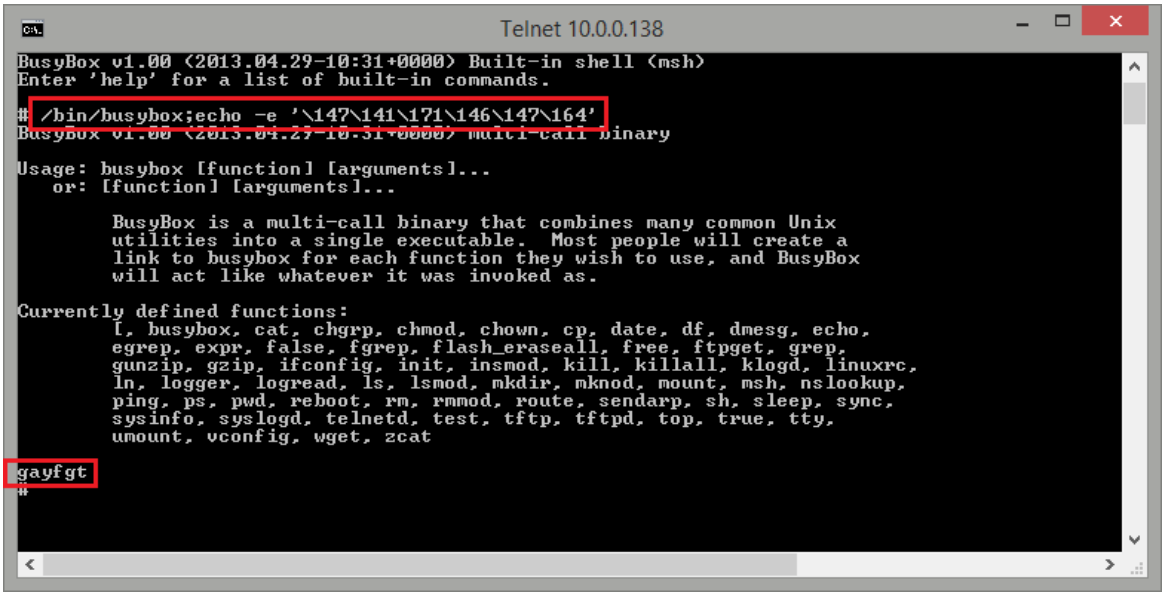
```
guest
login
changeme
1234
12345
123456
default
pass
password
```

במידה והייתה התחברות מוצלחת. תורץ הפקודה הבאה:

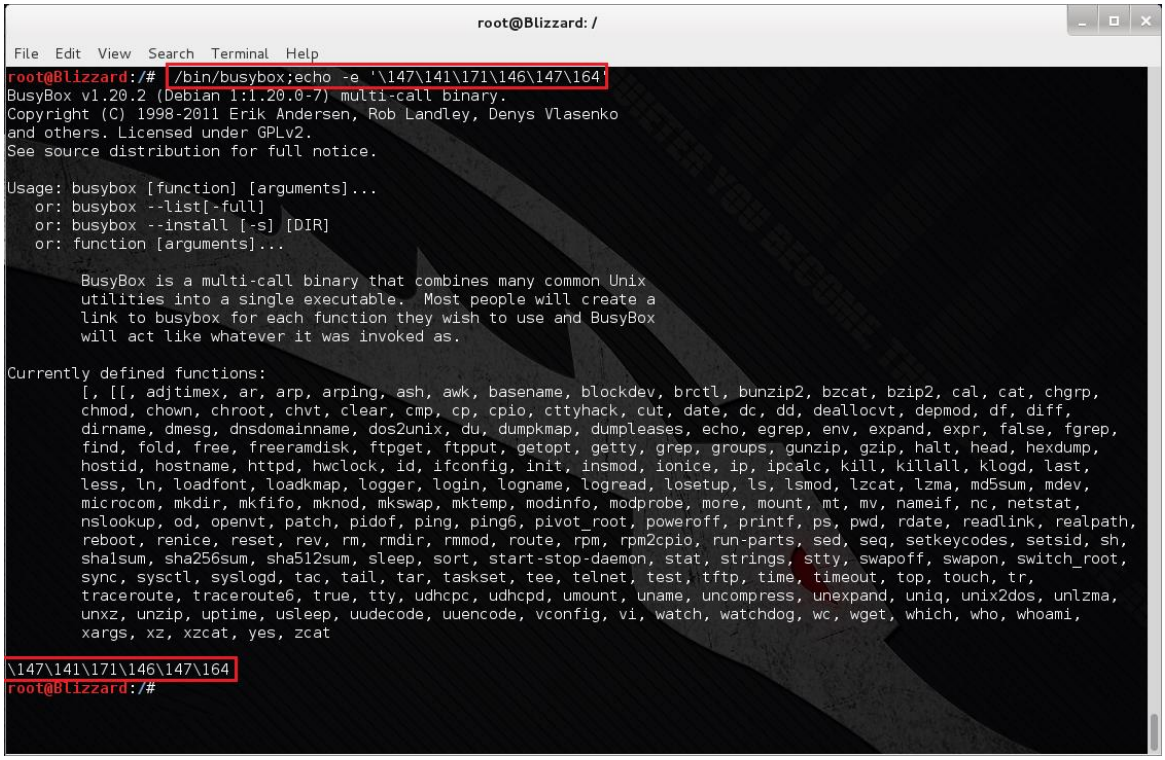
```
/bin/busybox;echo -e '\147\141\171\146\147\164'
```

הפקודה הנ"ל הינה בדיקת Fingerprinting האם אכן מדובר ברכיב תמים המריץ busybox אמיתי או ב-Honeypot שרק נועד לסמלץ את הסביבה. על רכיבים תמימים הפלט המצופה לקבל שולח לכתובת את המחרוזת "gayfgt".

לדוגמא:



ולעומת זאת, מחוץ ל-Busybox, הפקודה תחזיר:



הדבר נגרם בעקבות ההבדלים בין ה-Shell-ים השונים הקיימים במערכות השונות. הפקודה echo -e שמורצת בעזרת /bin/sh (מה שבדרך כלל רץ על רכיבי Embedded) מפרסרת מחרוזות עם סלאשים הפוכים אחרת מהצורה בה /bin/bash מפרסרת אותה, וכך ניתן לדעת האם אנחנו אכן מורצים בעזרת /bin/sh מה ש(לפי כותבי ה-Malware) מניח את הדעת שאנו אכן רצים על רכיב Embedded / מוריד את הסיכוי שמדובר ב-Honeypot. (בגרסאות שונות של ה-Malware מופיעות מחרוזות בדיקה אחרות אך העקרון זהה).

לאחר מכן, תורץ פקודת wget (ולעיתים אחריה גם פקודת tftp) שמטרתן להוריד את ה-Malware עצמו מאחד השרתים שבשליטת המפציפים ולהריצה.

אגב, בגרסאות שונות של אותו הכולירע ניתן לראות אף נסיונת תקיפה עם shellshock, כפי שפורסם בגליון ה-54 של Digital Whisper

- **HOLD** - הפקודה **HOLD** מאפשרת לתוקפים להפסיק תקיפת DoS עבור כתובת IP ספציפית לפרק זמן רצוי.
- **KILLATTK** - הפקודה **KILLATTK** תגרום לבוט לעצור את כלל התקיפות שמתבצעות כרגע.

- **HTTP, JUNK, UDP** - הפקודות **HTTP**, **JUNK** ו-**UDP** יגרמו לבוט ליזום שלושה סוגי מתקפות DoS שונות. בגרסאות שונות קיימת גם הפקודה "**TCP**" שתפקידה ליזום סוג נוסף של תקיפה. בעת תחילת התקיפה תשלח ליוזם התקיפה הודעה בסיגנון:

```
JUNK Flooding IP:POST for X seconds.
```

התגוננות

על מנת להתגונן ברמה הפרטית אנו ממליצים:

- לסגור את הממשקים שאינם דרושים. אין סיבה שממשק ה-Telnet או ממשק ה-SSH יהיה פתוח כברירת מחדל על מצלמות אבטחה. יש לפתוח ממשקים אלו לפרק זמן מוגבל ורק בעת הצורך.
- לשנות את הסיסמאות שמגיעות כברירת מחדל עם המערכות השונות. סיסמאות אלו הן וקטור חדירה מאוד נח ואינו דורש שום מחשבה מהצד התוקף, יש לשנותן לסיסמאות קשות לניחוש.
- לעבוד מאחורי NAT ולחשוף אך ורק ממשקים הנדרשים לנו בעת העבודה מרחוק. כך, גם אם שכחנו שירות פתוח או לשנות סיסמא דיפולטיבית - אותם השירותים אינם מנותבים מרשת האינטרנט.
- לא להגיד את המשפט הטפשי "למה שינסו לפרוץ לי? אני בסך הכל אדם פרטי, אני לא מעניין אף אחד". אז נכון - ככל הנראה אתה באמת לא מעניין אף אחד, אבל כח העיבוד והחיבור לרשת של רשת המצלמות שלך בהחלט מעניינים את מי שמנסה להגדיל בכל מחיר את רשת הבוטנטים שלו.

על מנת להתגונן ברמת הארגון:

- ליישם את כלל הסעיפים הנוגעים לרמה הפרטית, מהבחינה הזאת - אין הבדל בין האירועים.
- במידת האפשר - לאפשר התחברות למערכות הפנים-ארגוניות אך ורק באמצעות VPN.
- לעדכן תמיד את החוקים ב-IPS/IDS/FW הארגוני, ובפרט להוסיף את חוקי ה-YARA הבאים:

```
rule bashWorm {
	strings:
		$a = "JUNK Flooding %s:%d for %d seconds."
		$a2 = "UDP Flooding %s for %d seconds."
		$a3 = "UDP Flooding %s:%d for %d seconds."
		$a4 = "TCP Flooding %s for %d seconds."
		$a5 = "KILLATTK"
		$a6 = "REPORT %s:%s:"
		$a7 = "PING"
		$a8 = "PONG!"
		$a9 = "GETLOCALIP"
	condition:
		all of them
}
```

[נלקח מ-https://www.alienvault.com/open-threat-exchange/blog/attackers-exploiting-shell-shock-cve-2014-6721-in-the-wild]

סיכום

אנו מקווים כי הסיפור שלנו מראה עד כמה עולם ה-"Internet Of Things" יכול להיות מסוכן, ומקווים כי פרסום המקרה יעלה את המודעות לעניין. בימים אלו אנו עדים למתקפת DDoS נוספת המגיעה אלינו מעולם ה-IoT - הפעם מרכיבי NAS, ואכן, ניחשתם נכון - גם רכיבים אלה נפרצו על-ידי מתקפת Brute Force מבוססת מילון על אחד משירותי הניהול מרחוק שלהם.

אז בבקשה, לא משנה אם מדובר במצלמה, מקרר או נתב ביתי - סגרו את ממשקי הניהול שיכולים לפגוע בכם, שנו את סיסמאות ברירת המחדל שקיבלתם בעת ההתקנה של הרכיב, ותעבדו מאחורי NAT. אחרת - גם אתם תתווסו לסטטיסטיקה של צוות Incapsula...