مقدمه ای بر امنیت سایبری در IoT

محسن طهماسبی

آذر ۱۴۰۳

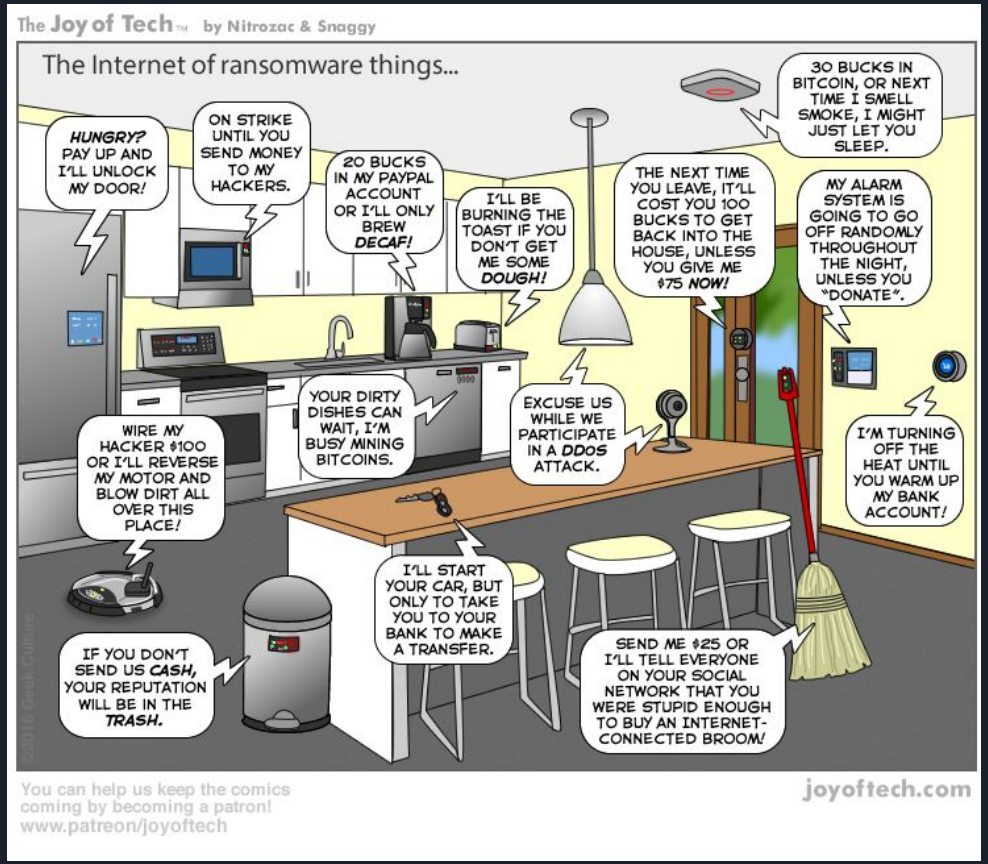
این ارائه با فونت وزیر متن ساخته شده

به یاد صابر راستی کردار

چند نفر از شما به امنیت سایبری علاقه‌مندید؟

- چرا اهمیت دارد؟
- چگونه تهدید می‌کند؟
- چه باید کرد؟

چرا؟


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech
joyoftech.com

چرا؟

- حضور روز افزون در زندگی روزمره
- وابستگی
- کاربرد های حساس (مانند قفل در)
- امکان گسترش آلودگی

خطرات

- شنود، نقض حریم خصوصی و درز اطلاعات
- خرابکاری (Sabotage)
- ربایش کنترل

شنود، نقض حریم خصوصی و درز اطلاعات

- سوءاستفاده از سنسور های دستگاه (دوربین، میکروفون)
- دسترسی به اطلاعات و تنظیمات خصوصی
- درز متادیتا

خرابکاری (Sabotage)

- باج افزار
- دستورات آسیب‌زا
- آسیب به Firmware و بریک کردن

ربایش کنترل

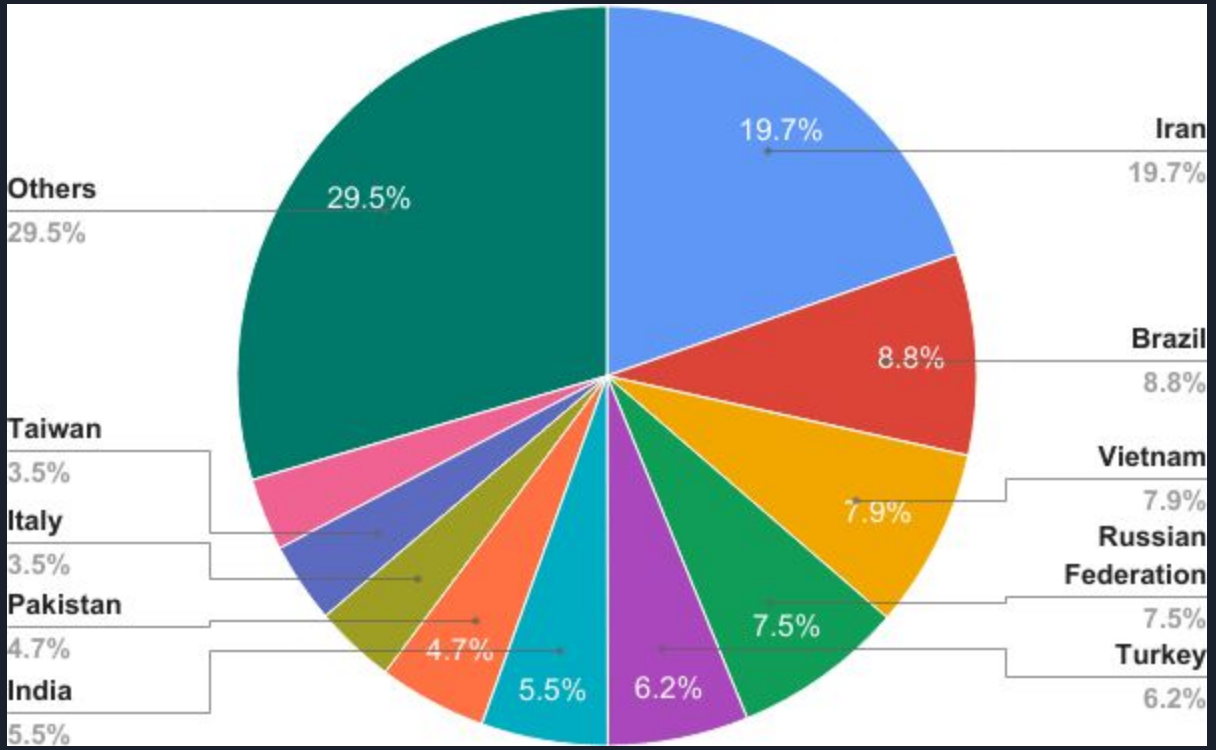
- شنود شبکه
- آلودگی شبکه و Lateral Movement
- اجرای حملات DDoS
- اسکن اینترنت و پخش آلودگی

چگونه؟

Mirai & Mirai-like (2016-Now)

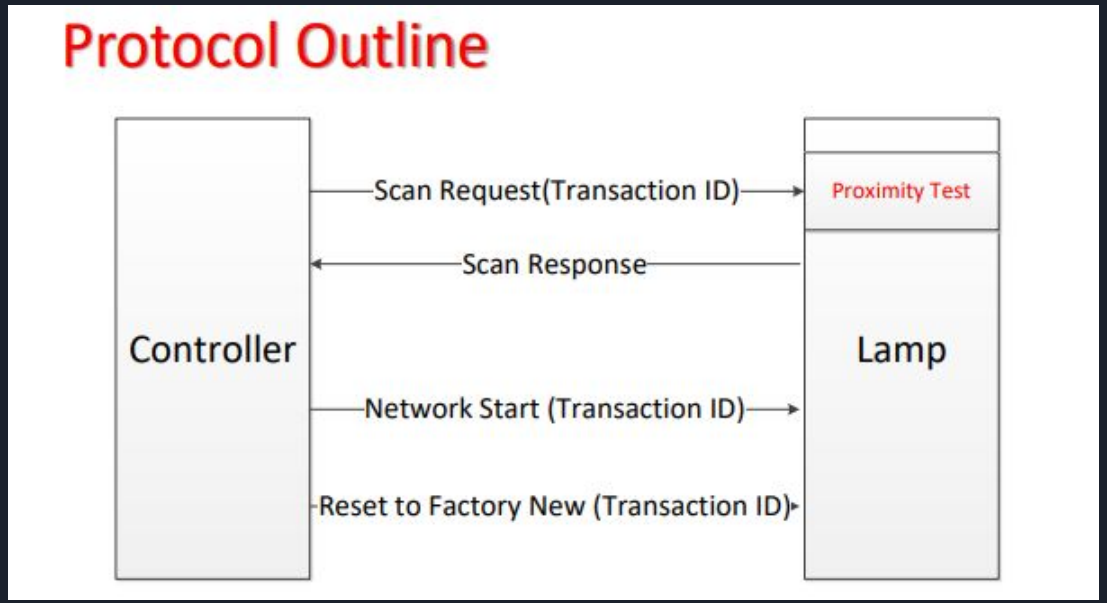
- هدف قرار دادن دستگاه های آسیب پذیر یا با پسورد ضعیف
- اضافه کردن دستگاه به بات نت
- اسکن اینترنت و شبکه برای اهداف جدید
- اجرای حملات DDoS

بدافزار Hajime در ایران



[1]

ZigBee Chain Reaction (2017) [2]



- آسیب پذیری در پیاده سازی پروتکل ZigBee در لامپ‌های Philips Hue
- ارسال کامند ریست فکتوری

ZigBee Chain Reaction (2017)

- بررسی رمزنگاری Firmware ها
- استخراج کلید با حمله Side Channel
- ساخت Firmware آلوده و پخش از طریق آپدیت OTA

ZigBee Chain Reaction (2017)

- قابلیت کنترل کامل لامپ
- قابلیت گسترش آلودگی به لامپ های اطراف
- قابلیت Brick کردن لامپ
- ایجاد واکنش زنجیره ای و آلوده کردن کل یک شهر

Nooie Baby Monitor (2022) [3]

- عدم اعتبارسنجی در MQTT Server
- قابلیت ارسال دستور به دوربین ها
- قابلیت تعیین فید ویدئو

چه باید کرد؟

اشکالات امنیتی

- اشکالات طراحی
- اشکالات پیاده سازی

اشکالات طراحی

- مکانیزم ناامن احراز هویت
- مکانیزم ناامن ارسال و دریافت دستور
- مکانیزم ناامن آپدیت
- طراحی اعتماد محور
- طراحی کلاینت محور

اشکالات پیاده سازی

- آسیب پذیری های حافظه
- عدم Sanitize صحیح ورودی ها
- زیرساخت مرکزی ناامن
- استفاده از Library های ناامن یا قدیمی
- رمزنگاری ضعیف
- پیاده سازی غلط پروتکل ها

امن سازی

- ذهنیت امنیت سایبری
- طراحی و پیاده سازی استاندارد
- برنامه نویسی امن یا استفاده از زبان های Memory Safe
- آگاهی از اشکالات امنیتی متداول
- امنیت چند لایه
- امنیت زیرساخت
- معماری Zero Trust

ممنونم!

Twitter/X: moh53n_fa
Email: moh53n@moh53n.ir

References

[1]: https://securelist.com/hajime-the-mysterious-evolving-botnet/78160/

[2]: https://eyalro.net/publication/rosw17.html

[3]: https://www.bitdefender.com/en-gb/blog/hotforsecurity/nooie-baby-monitor-vulnerabilities-let-attackers-intercept-live-feed-and-recordings-in-the-cloud