RSA®Conference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: SEM-M03D

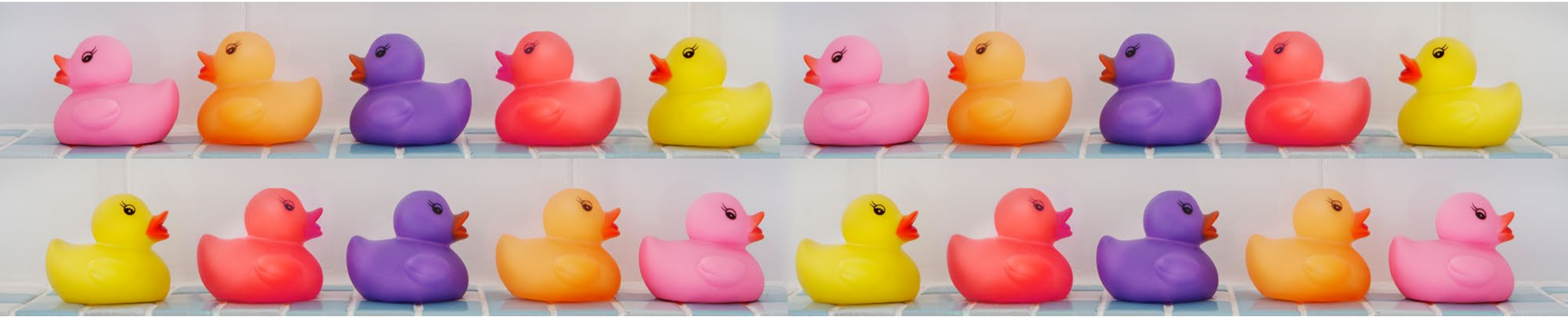
Profiting from Hacked IoT Devices: Coin Mining, Ransomware, Something Else?

Candid Wueest

Threat Researcher
Symantec
@MyLaocoon

#RSAC

What do cyber criminals do with 100,000 IoT bots?



Different motivations for different attackers

Profit/Financial

- Loot online accounts
- Steal credit card details
- Extortion & scams
- Crypto coin mining

Espionage/Sabotage

- Steal company secrets
- Monitor communication
- Sabotage of critical targets
- Wipe company systems

Ideology/Personal

- Disclose scandals & leaks
- Hacking for fun & fame
- Statements e.g. DDoS
- Social media bots / propaganda

How devices get infected…

…is not part of this talk.

75% of infections are on routers | avg. of 6 IoT devices / house*

Infection vectors:

- IoT default credentials
- Exploits (service & protocol)
- Prescanned list e.g. Shodan
- LAN attacks e.g. DNS rebinding/UPnP
- Supply chain/second hand

Most common IoT threats:

Threat name	Percentage	Main purpose
LightAidra	31.3%	DDoS
Kaiten	31.0%	DDoS
Mirai	17.8%	DDoS/Misc
Downloader	11.7%	Misc
Gafgyt/BashLite	1.7%	DDoS

(* Norton Core data (US))

Possible scenarios for cyber criminals

- DDoS attacks
- Spam attacks
- Cryptocurrency mining
- Ransomware/locker
- Blackmail/extortion
- Pranks/nuisance
- Information stealing
- Click fraud/ad fraud
- Premium services
- Network sniffing
- Attack other devices
- Proxy network

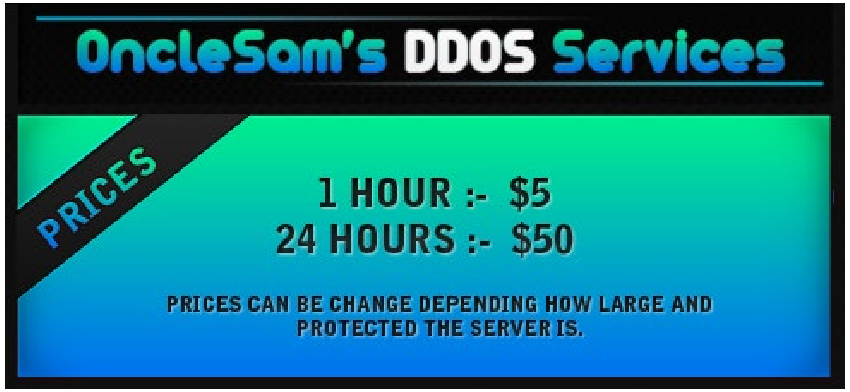
DDoS with IoT

⊕ Profitability
⊕⊕ Feasibility
⊖ Stealth
⊕⊕ Prevalence

- **Most common payload (e.g. Mirai)**
  - Very noisy (even when pulsed)→ devices will get blocked
- **IoT protocols can be used as DoS amplification**
  - E.g. Constrained Application Protocol (CoAP) & MQTT

Profits are medium:

- Not expensive to rent
- Often used for extortion
- $5-10K/month for stresser service



OncleSam's DDOS Services

PRICES

1 HOUR :- $5
24 HOURS :- $50

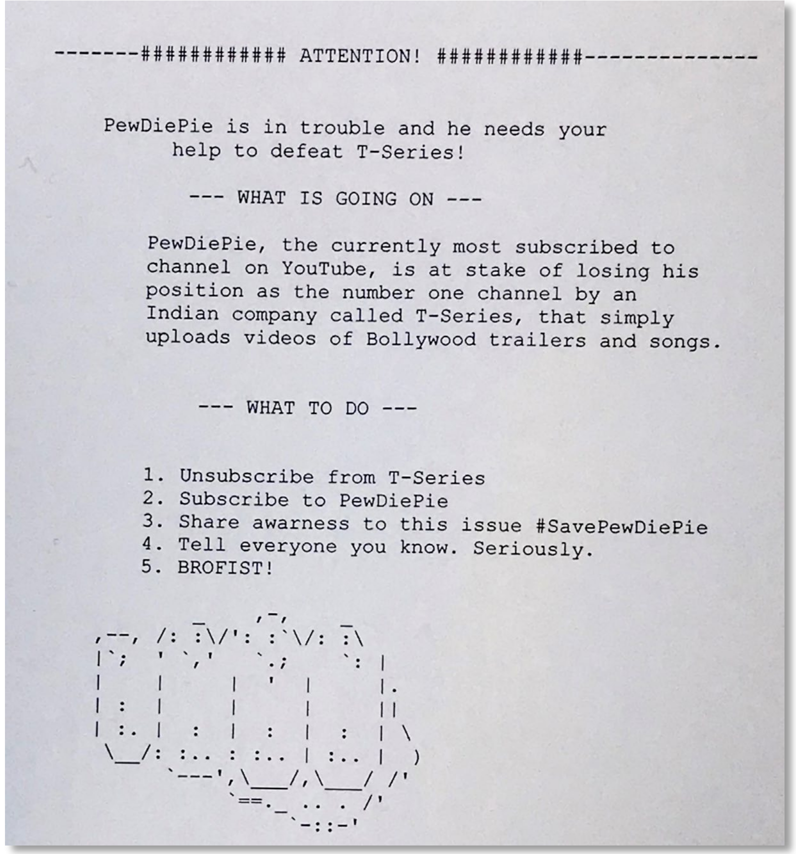
PRICES CAN BE CHANGE DEPENDING HOW LARGE AND PROTECTED THE SERVER IS.

Spamming through IoT

- **Sending typical spam emails**
  - Feasible, but little profit (e.g. ProxyM)
- **Hijack printer to spit out spam**
  - YouTuber mass rally in 2018
- **Music/video spam**
  - «RickRoll», but with advertisements
  - YouTuber mass rally in 2018 on TVs

Profits are low:

- Not expensive
- Kelihos (not IoT): $500 to send 1M spam



```
-------############ ATTENTION! ############--------------

      PewDiePie is in trouble and he needs your
           help to defeat T-Series!

             --- WHAT IS GOING ON ---

         PewDiePie, the currently most subscribed to
         channel on YouTube, is at stake of losing his
         position as the number one channel by an
         Indian company called T-Series, that simply
         uploads videos of Bollywood trailers and songs.


              --- WHAT TO DO ---


         1. Unsubscribe from T-Series
         2. Subscribe to PewDiePie
         3. Share awarness to this issue #SavePewDiePie
         4. Tell everyone you know. Seriously.
         5. BROFIST!

        _    ,-,    _
,--, /: :\/': :`\/: :\
|`;  ' `,'   `.;    `: |
|    |     |  '  |     |.
| :  |     |     |     ||
| :. |  :  |  :  |  :  | \
 \__/: :.. : :.. | :.. |  )
      `---',\___/,\___/ /'
           `==._ .. . /'
                `-::-'
```

⊖⊖ Profitability

⊕ Feasibility

⊖ Stealth

⊖⊖ Prevalence

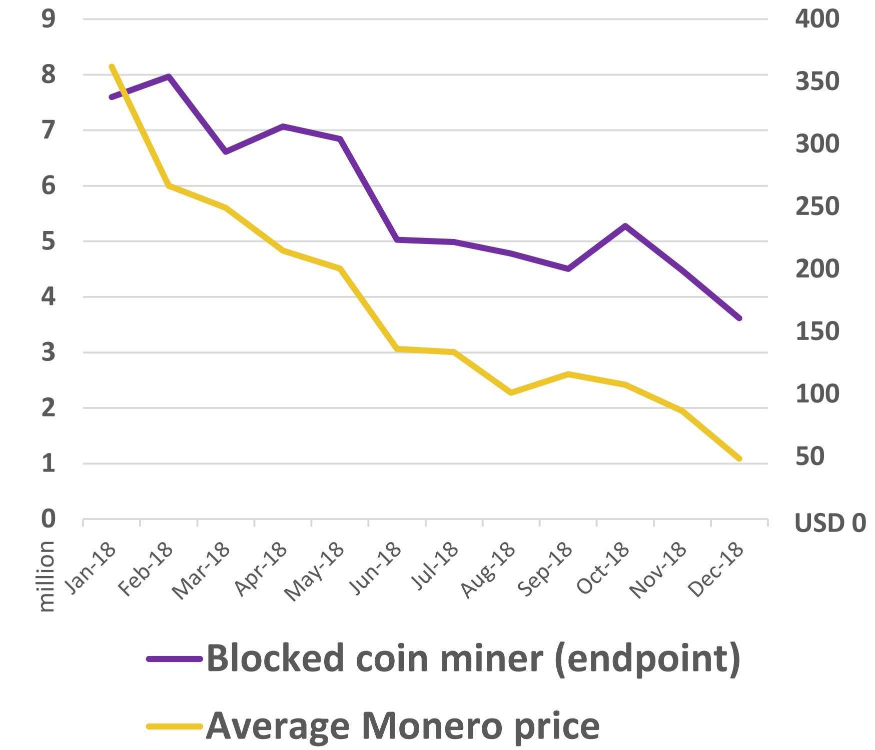
Crypto coin mining on IoT

🟡 Profitability
⊖ Feasibility
⊕ Stealth
⊕⊕ Prevalence

- **Limiting factors**
  - Not all devices have enough performance
  - Crypto coin prices are down
- **Easy to cash out «anonymously»**
- **Router can inject script into traffic**
  - Mining is done on non-IoT devices

Profits are medium-low:

- Satori: ETH $35/month
- Hide’n’Seek: XMR $25/month (300H/S/1k bots)
- Smominru (not IoT): XMR $25,000+/month

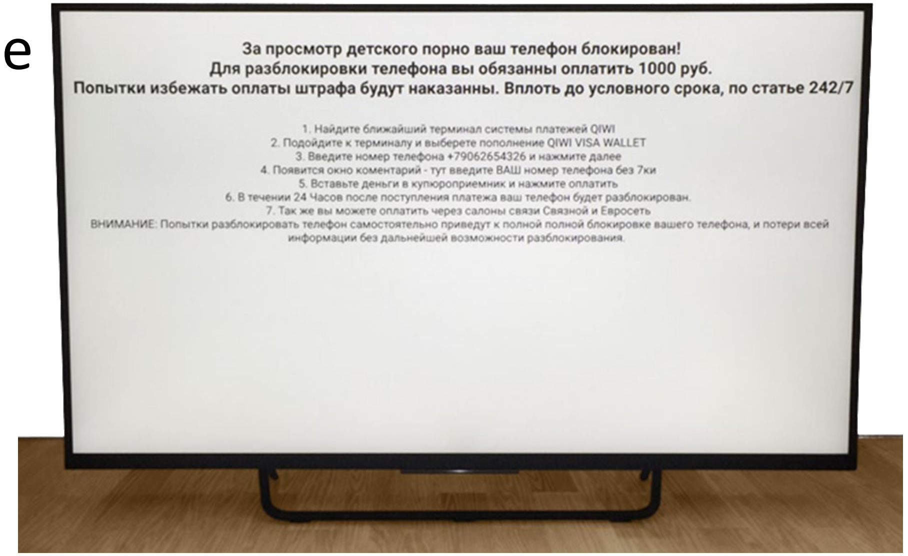


Ransomware/locker on IoT

⊕ Profitability
⊖ Feasibility
⊖⊖ Stealth
⊖⊖ Prevalence

Would you pay $500 to unlock a $10 light bulb?

- **Needs notification method (display or hub app)**
  - Does not work for all devices
  - Rarely has data/services that could be held hostage
- **Works, for example, on SmartTVs (2015)**
  - Only a hand full of real world cases



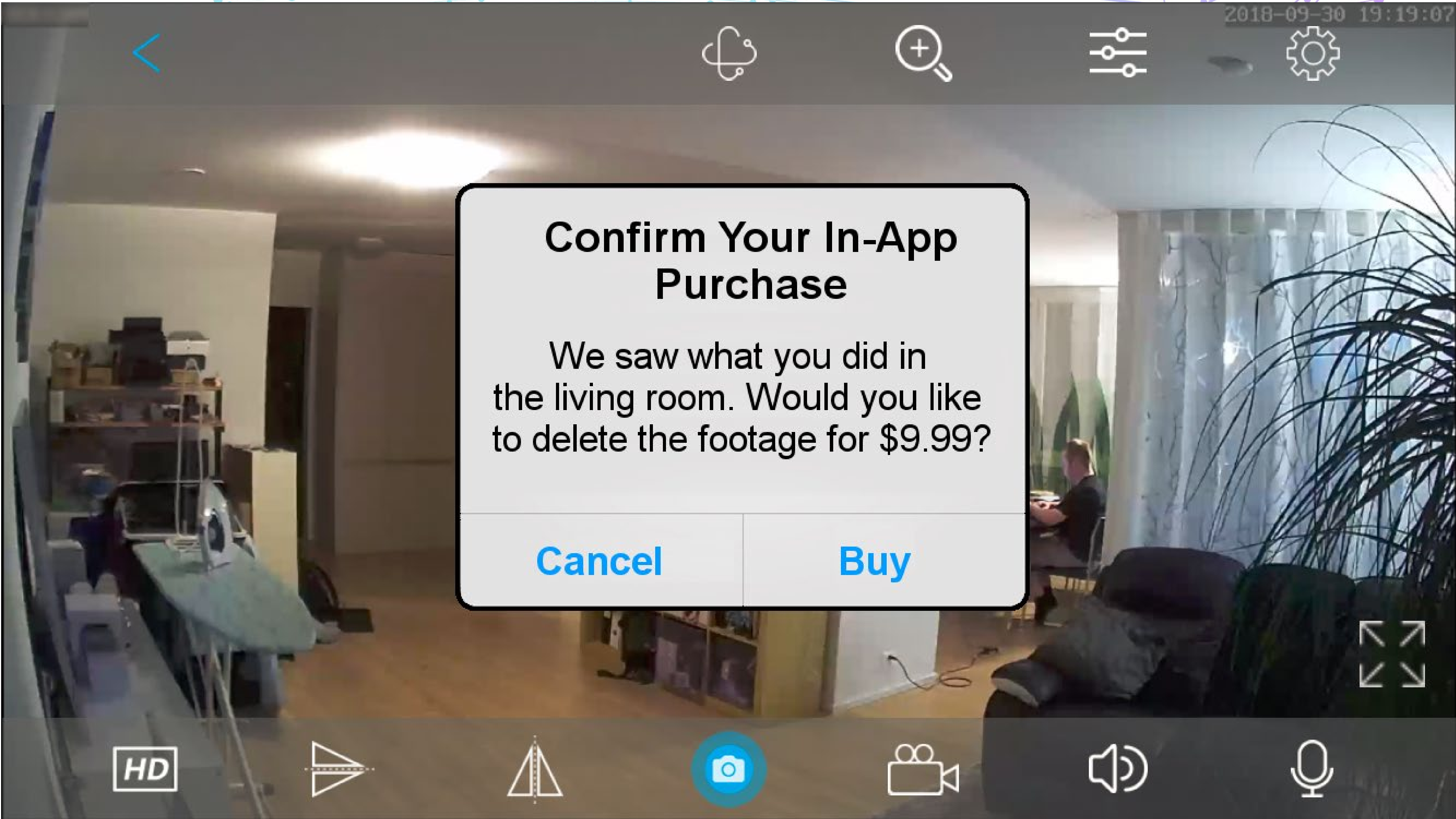
За просмотр детского порно ваш телефон блокирован!
Для разблокировки телефона вы обязанны оплатить 1000 руб.
Попытки избежать оплаты штрафа будут наказанны. Вплоть до условного срока, по статье 242/7

1. Найдите ближайший терминал системы платежей QIWI
2. Подойдите к терминалу и выберете пополнение QIWI VISA WALLET
3. Введите номер телефона +79062654326 и нажмите далее
4. Появится окно коментарий - тут введите ВАШ номер телефона без 7ки
5. Вставьте деньги в купюроприемник и нажмите оплатить
6. В течении 24 Часов после поступления платежа ваш телефон будет разблокирован.
7. Так же вы можете оплатить через салоны связи Связной и Евросеть

ВНИМАНИЕ: Попытки разблокировать телефон самостоятельно приведут к полной полной блокировке вашего телефона, и потери всей информации без дальнейшей возможности разблокирования.

Could be profitable:

- 100 paid infections at $100 = $10K/month



Confirm Your In-App Purchase

We saw what you did in the living room. Would you like to delete the footage for $9.99?

Blackmail/extortion through IoT

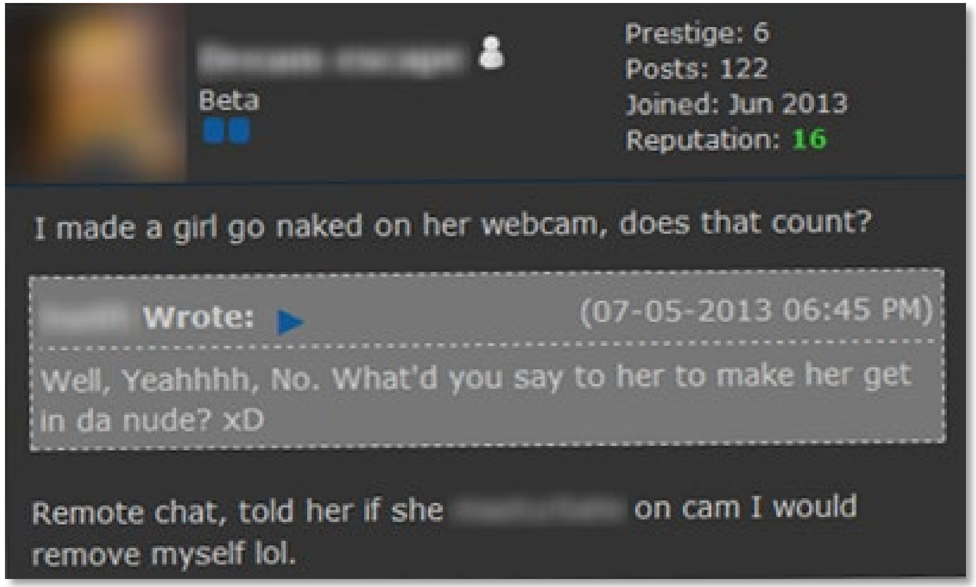
- 🟡 Profitability
- ⊕ Feasibility
- ⊕ Stealth
- ⊖ Prevalence

- **Video/voice recording → «I know what you did»**
  - Toy doll/voice assistant with microphone recording
  - Sextortion with video from CCTV
  - Use social media account to ruin reputation
- **Location tracking**
  - Fitness tracker reveals military location
  - Dashcam shows cheating husband
- **Blackmailing the vendor**
  - Pay or you get bad press
  - Pay or people die (medical devices)

Nuisance and pranks on IoT

⊖ ⊖ Profitability
⊕ ⊕ Feasibility
⊕ Stealth
🟡 Prevalence

- **Playing videos or songs on IoT devices**
  - «RickRoll» for a laugh
  - Profitable, if playlist has ads or affiliate program
- **IP cameras & baby monitors**
  - Voyeurism, trolling, or burglar reconnaissance
  - E.g. false missile alarm



[redacted]
Beta

Prestige: 6
Posts: 122
Joined: Jun 2013
Reputation: 16

I made a girl go naked on her webcam, does that count?

> [redacted] Wrote: (07-05-2013 06:45 PM)
>
> Well, Yeahhhh, No. What'd you say to her to make her get in da nude? xD

Remote chat, told her if she [redacted] on cam I would remove myself lol.

Profits are low, they do it for the laughs

Example of data-leaking light bulb

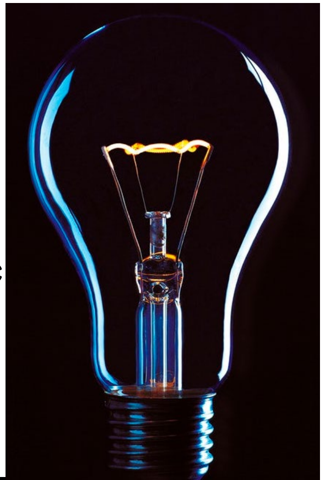
Un-encrypted requests revealing user details and MD5 hash of password (unsalted)

POST /changeDeviceName

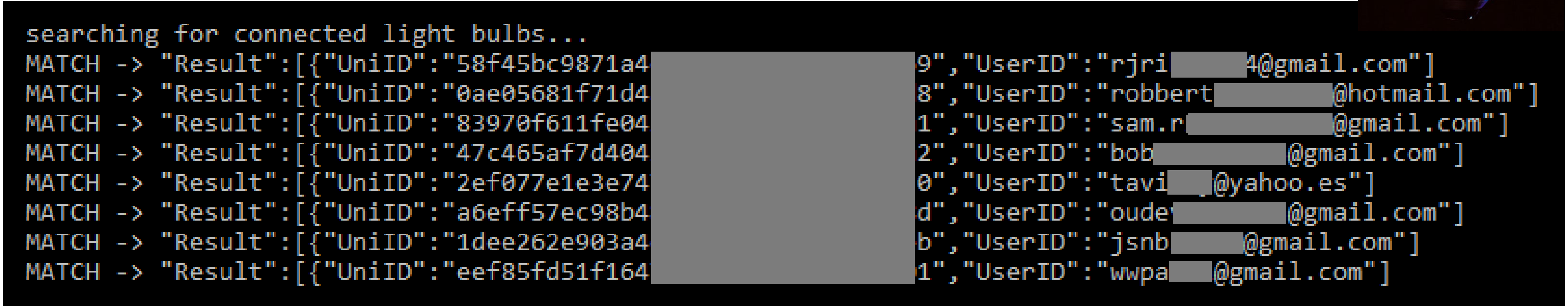
"UserID":«a-test-account@*********»,

"Password":"9a323c5a74e4e3de45968c732157f0de",

"Devices":[{"deviceName":"Bulb LivingRoom", "macAddress":"DC4F22******



Service allows enumeration of all users and remote takeover of device



```
searching for connected light bulbs...
MATCH -> "Result":[{"UniID":"58f45bc9871a4[redacted]9","UserID":"rjri[redacted]4@gmail.com"]
MATCH -> "Result":[{"UniID":"0ae05681f71d4[redacted]8","UserID":"robbert[redacted]@hotmail.com"]
MATCH -> "Result":[{"UniID":"83970f611fe04[redacted]1","UserID":"sam.r[redacted]@gmail.com"]
MATCH -> "Result":[{"UniID":"47c465af7d404[redacted]2","UserID":"bob[redacted]@gmail.com"]
MATCH -> "Result":[{"UniID":"2ef077e1e3e74[redacted]0","UserID":"tavi[redacted]@yahoo.es"]
MATCH -> "Result":[{"UniID":"a6eff57ec98b4[redacted]d","UserID":"oude[redacted]@gmail.com"]
MATCH -> "Result":[{"UniID":"1dee262e903a4[redacted]b","UserID":"jsnb[redacted]@gmail.com"]
MATCH -> "Result":[{"UniID":"eef85fd51f164[redacted]1","UserID":"wwpa[redacted]@gmail.com"]
```

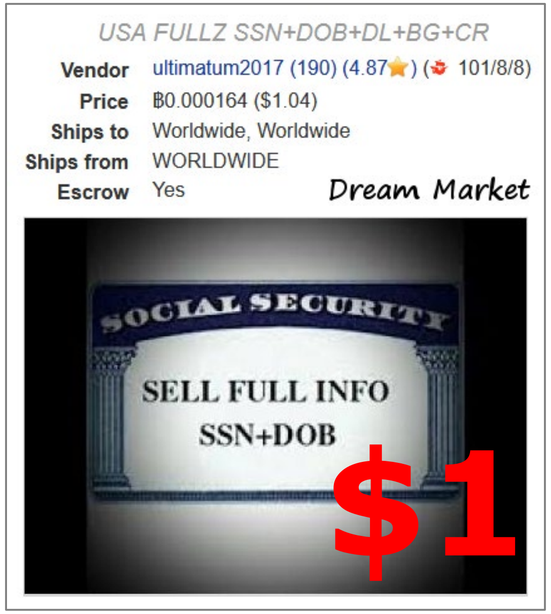
Information stealing from IoT devices

● Profitability
⊕⊕ Feasibility
⊕ Stealth
● Prevalence

- **Emails, passwords, Wi-Fi keys,… → further attacks**
- **Credit cards, credentials,… → sell on underground forums**
  - Usually entered into app and not the IoT device itself
- **Private data → Leaked to the cloud or on the device**
  - Blackmail or personalized spam
- **Sell data on dark web in bulk**
  - Could be sold to advertisers (even by vendor)
  - Profit by using it for fraudulent warranty cases

Profits are low-medium:

- Often easier to get the data from the cloud directly



USA FULLZ SSN+DOB+DL+BG+CR

Vendor	ultimatum2017 (190) (4.87★) (101/8/8)
Price	Ƀ0.000164 ($1.04)
Ships to	Worldwide, Worldwide
Ships from	WORLDWIDE
Escrow	Yes

Dream Market

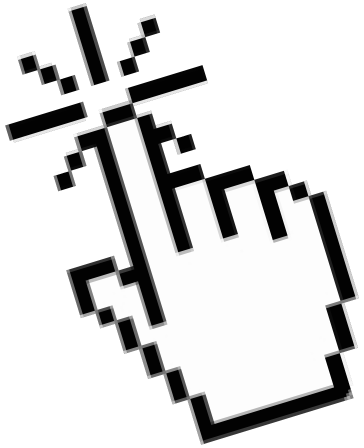
Click fraud/ad fraud through IoT

➕ Profitability
➕➕ Feasibility
➕ Stealth
➖ Prevalence

- Use IoT device to click ads or view videos
- Not much bandwidth or CPU power needed
- Not always easy to set up and cash out

Profits can be high:

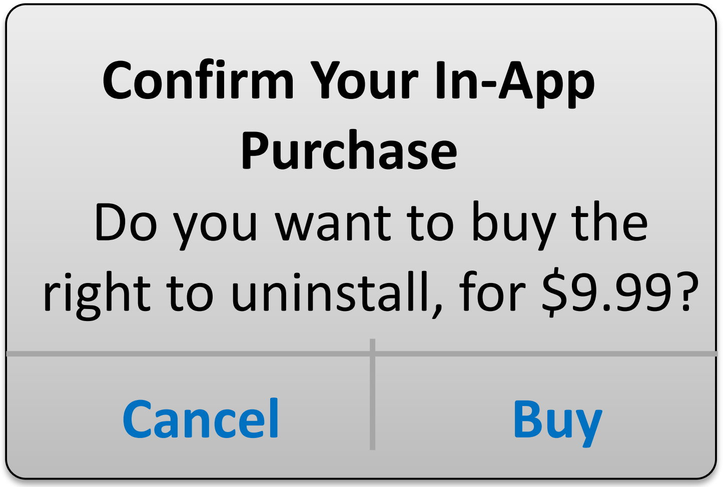
- Bamital: (not IoT) 1.5 million bots → $75K/month
- HummingBad: 60 million mobiles → $10K/month



Premium services

⊕ Profitability
⊖⊖ Feasibility
🟡 Stealth
⊖⊖ Prevalence

- **Premium SMS and calls**
  - Devices rarely have a phone line connected to them
- **Concealed in-app purchases**
  - E.g. Alexa in-skill purchases, needs exploit or social engineering
  - Can be addressed by the platform vendor
- **Sell «fake» services**
  - Buy this app to get faster music streams



Confirm Your In-App Purchase

Do you want to buy the right to uninstall, for $9.99?

Profits can be high:

- Difficult to cash out over a long time

RSA®Conference2019

Targeted attack groups using IoT

Sniffing network traffic

- 🟡 Profitability
- ⊖ Feasibility
- ⊕⊕ Stealth
- ⊖ Prevalence

Use compromised IoT devices to sniff network traffic

VPNFilter group

- Compromised various routers
- Persistent – reboot will not disinfect
- Has multiple payload modules:
  - MITM attacks
  - Intercept SCADA Modbus traffic
  - Local network scanner
  - "Brick" a device → sabotage

MikroTik campains

- Enable RouterOS feature to redirect traffic to remote IP address
- Could be sold as access to networks
- Hidden infection, that can re-infect PCs in the local network

Stepping stone/pivoting

- ➕ Profitability
- 🟡 Feasibility
- 🟡 Stealth
- ➖ Prevalence

Use compromised IoT devices to attack other devices

Slingshot group

- Add malicious IPv4.dll to compromised MikroTik router
- Official administration tool (Winbox Loader) downloads planted DLL and runs it
- Router infects PC with malware

VPNFilter group

- Inject malicious JavaScript into network traffic for other devices

Satori

- Search and substitute Claymore miner wallet address for their own
- Change DNS server → phishing,…

Hiding origin with proxies

- 🟡 Profitability
- 🟡 Feasibility
- ⊕ Stealth
- 🟡 Prevalence

Use compromised IoT devices to hide traffic origin

Inception Framework group

- Hiding activity behind compromised routers that act as proxies
- Chaining multiple devices
- Cleaning up afterwards

RouterOS campaigns

- Creating network of Socks proxies
- Using built-in features
- 240,000+ devices compromised

→ Can be used for spam, click fraud, credential stuffing, port scaning,…

Summary of the scenarios

Attack method	Profitability	Comment	Trend
DDoS attacks	⊕	Still growing in size - simple	⬆
Spam attacks	⊖ ⊖	Not the easiest way to spam	⬇
Cryptocurrency mining	●	Depends on the coin price	➡
Ransomware/locker	⊕	Might work on some devices	⬆
Blackmail/extortion	●	Does not scale well – depends	➡
Pranks/nuisance	⊖ ⊖	Not done by cyber criminals	➡

(Trends based on current ecosystem)

Summary of the scenarios

Attack method	Profitability	Comment	Trend
Information stealing	🟡	Done because it’s simple	⬆
Click fraud	⊕	Often overlooked - profitable	⬆
Premium services	⊕	Difficult to conduct	⬇
Sniffing network traffic	🟡	Difficult with SSL/TLS	⬇
Pivoting/attacking LAN	⊕	Infecting attached computers	⬆
Proxy	🟡	Not very lucrative, but useful	➡

(Trends based on current ecosystem)

Conclusion

Many ways to profit from compromised IoT devices

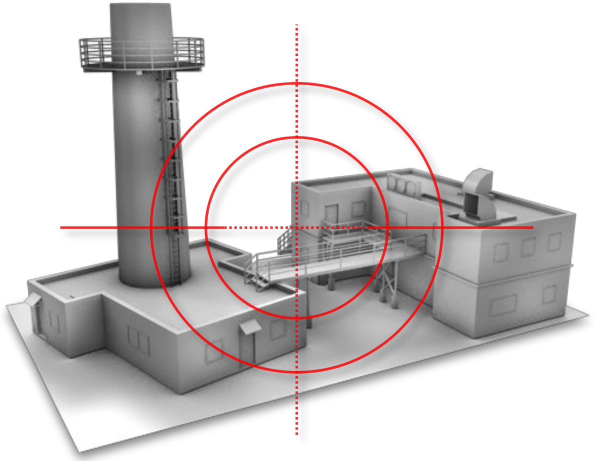
- Not all attacks work for all IoT device classes equally
- Routers are the most interesting target
- Interest in IoT from targeted attack groups is growing

DDoS, coin mining, and ad fraud are most likely in the near future

The «other» IoT devices

Other groups of devices have different risk profiles

- **Medical devices**
  - Various cases of pace makers or insulin pumps being hacked by researchers
- **Industrial IoT**
  - Attacked for sabotage and extortion (needs plant knowledge)
- **Smart cities**
  - Change smart meter energy bill, manipulate transmissions,...
- **Physical security devices** (e.g. smart doors)
  - Could be hacked by thieves, but does not scale



Apply What You Have Learned

Next week you should:

- Identify all IoT devices you have in use
- Reboot each of them

In the near future you should:

- Review the configuration of each IoT device
- Make sure that they are getting updated
- Monitor for unusual behavior and secure them

RSAConference2019

Thank you for your attention!

Candid Wueest

Threat Researcher
Symantec
@MyLaocoon