



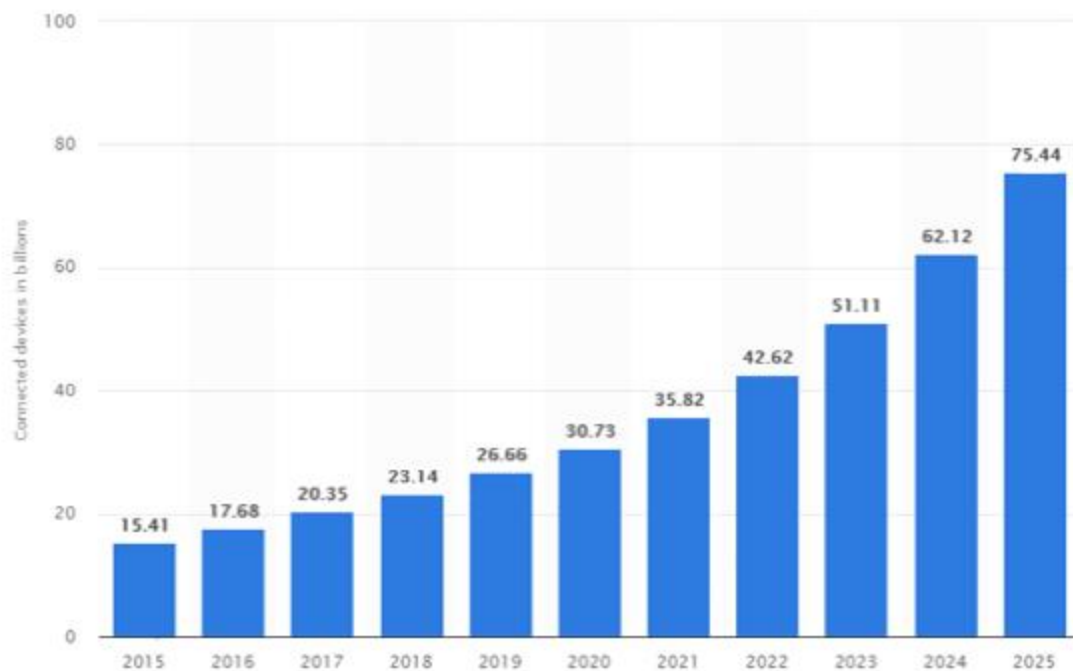
Hack-A-Home

Technology & Telecommunications > Consumer Electronics

PREMIUM

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025

(in billions)



DOWNLOAD



PDF



XLS



PNG



PPT

Sources

[→ Show sources information](#)[→ Show publisher information](#)

Release date

November 2016

Region

Worldwide

Survey time period

2015 to 2016

Supplementary notes

* Forecast data for 2017 to 2025

[Additional Information](#)

© Statista 2021

[Show source](#)

Smart Plug Users BEWARE: Hackers Can Use Them to SNEAK Into Your Home Network

By PJ Pierce, Tech Times | 23 May 2021, 08:05 am

Smart plug users have been warned to be careful when using these very useful doodads, because they might become cybersecurity risks under certain circumstances.



AMY GREENBERG SECURITY 11.04.2019 02:00 PM

Hackers Can Use Lasers to 'Speak' to Your Amazon Echo or Google Home

By sending laser-powered "light commands" to a smart assistant, researchers could force it to unlock cars, open garage doors, and more.



'I'm in your baby's room': A hacker took over a baby monitor and broadcast threats, parents say



First Look MAN HACKS WIRELESS CAMERA



• This article is more than 6 months old

Advertisement

Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs

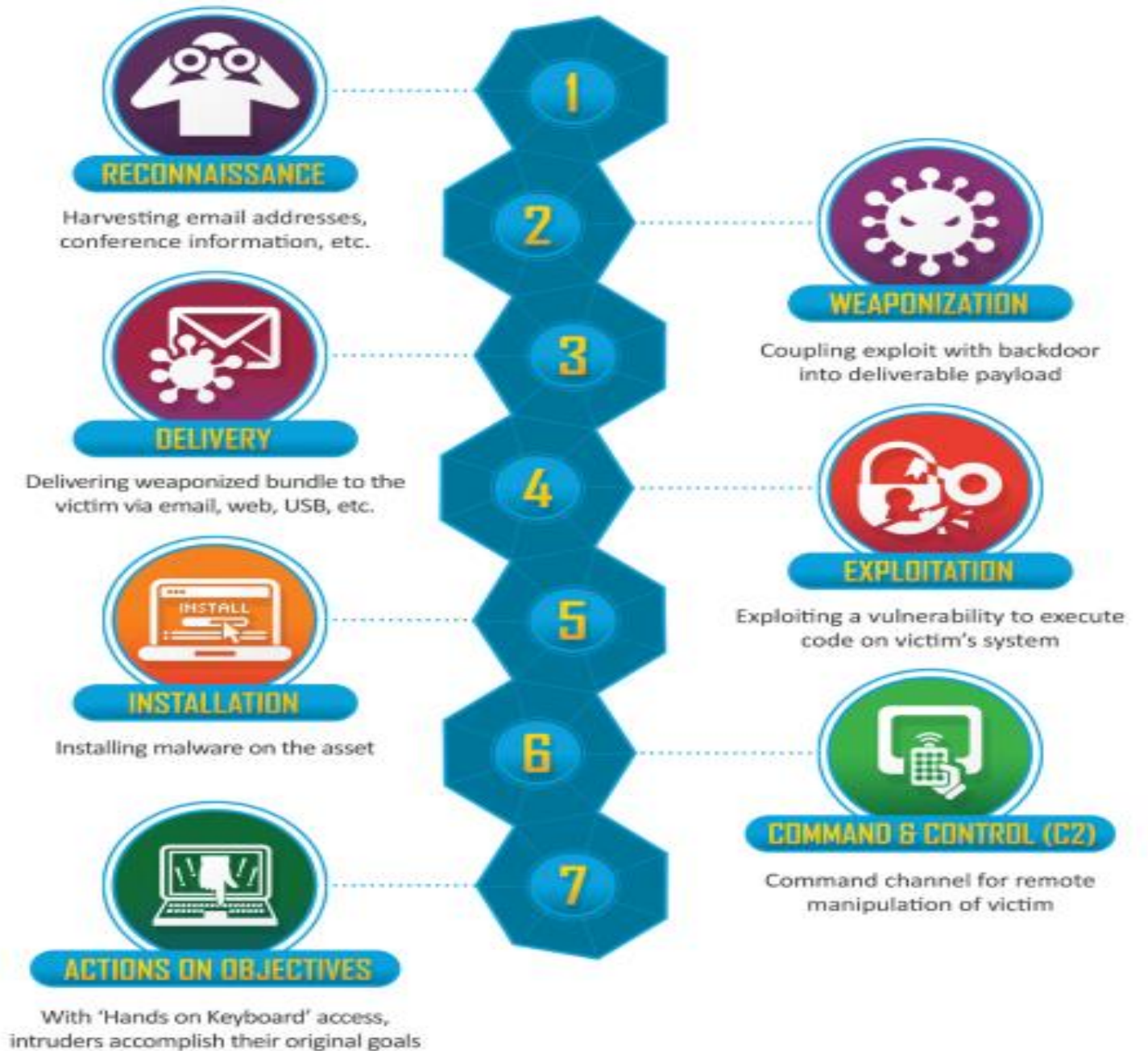
Class action claims weak security allowed hackers to take over the smart cameras used on doorbells and in homes





Internet of Things (lot) devices chosen


Cyber Kill Chain (CKC) Framework







1. Reconnaissance



merkury 1080p hack


×

🔍






AllShoppingImagesVideosNewsMoreTools


About 539,000 results (0.85 seconds)

[https://github.com › guino › Merkury720](https://github.com/guino/Merkury720)

[guino/Merkury720: Root and Customization for ... - GitHub](#) 














Merkury 720 Smart Home Camera root and customization ... and files to Root(hack) and

| | | | |
|---|------------------|-------------------|---|
|  guino | Update README.md | 55e468f on Feb 24 |  7 commits |
|  img | Added images | 5 months ago | |
|  mmc | Added mmc files | 5 months ago | |
|  README.md | Update README.md | 5 months ago | |

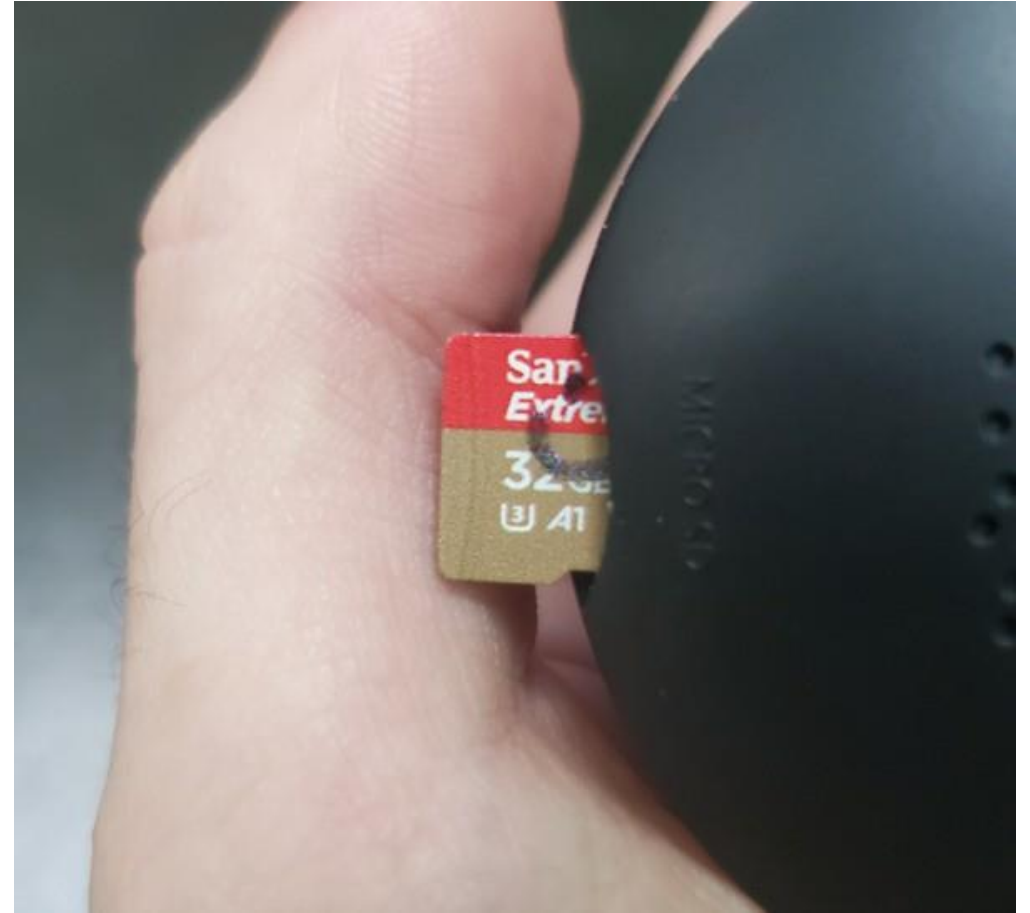
 README.md

Merkury1080P (CW017) Rooting and Customization

2. Weaponization

| Name | Date modified | Type | Size |
|--|------------------|---------------------|------|
|  cgi-bin | 7/8/2021 7:37 PM | File folder | |
|  busybox | 7/8/2021 7:37 PM | File | 1 KB |
|  custom.sh | 7/8/2021 7:37 PM | SH File | 1 KB |
|  env | 7/8/2021 7:37 PM | File | 1 KB |
|  httpd.conf | 7/8/2021 7:37 PM | CONF File | 1 KB |
|  index.html | 7/8/2021 7:37 PM | Firefox HTML Doc... | 2 KB |
|  initrun.sh | 7/8/2021 7:37 PM | SH File | 1 KB |
|  jpeg-arm | 7/8/2021 7:37 PM | File | 8 KB |
|  passwd | 7/8/2021 7:37 PM | File | 1 KB |
|  ppsFactoryTool.txt | 7/8/2021 7:37 PM | TXT File | 1 KB |
|  ppsMmcTool.txt | 7/8/2021 7:37 PM | TXT File | 1 KB |
|  set | 7/8/2021 7:37 PM | File | 1 KB |
|  upload.html | 7/8/2021 7:37 PM | Firefox HTML Doc... | 1 KB |

3. Delivery



4. Exploitation

← → ↻ 🏠 🛡️ 🔒 192.168.50.110:8090/proc/cmdline

```
mem=64M console=ttySAK0,115200n8 loglevel=10  
mtdparts=spi0.0:256k(bld),64k(env),64k(enc),64k(sysflg),3m(sys),4032k(app),640k(cfg)  
ppsAppParts=5 ip=0 - ip=30;/mnt/mmc01/initrun.sh)&:::::;date>/tmp/hack;(sleep
```


← → ↻ 🏠 🛡️ 🔒 192.168.50.110:8090/proc/self/root/mnt/mmc01/hack

done

5. Installation

| USB Drive (E:) > home > app | | | |
|-----------------------------|-------------------|------|----------|
| Name | Date modified | Type | Size |
| ppsapp | 2/7/2021 11:15 AM | File | 2,659 KB |
| ppsdsry | 2/7/2021 11:15 AM | File | 237 KB |

| Name | Date modified | Type | Size |
|--------------------|--------------------|---------------------|----------|
| bin | 7/8/2021 11:51 PM | File folder | |
| cgi-bin | 7/8/2021 7:37 PM | File folder | |
| etc | 12/31/2015 3:00 PM | File folder | |
| home | 12/31/2015 3:00 PM | File folder | |
| lib | 12/31/2015 3:00 PM | File folder | |
| sdrec | 7/8/2021 11:52 PM | File folder | |
| busybox | 7/8/2021 7:39 PM | File | 1,084 KB |
| custom.sh | 7/8/2021 8:14 PM | SH File | 1 KB |
| env | 7/8/2021 7:38 PM | File | 1 KB |
| hack | 12/31/2015 3:00 PM | File | 1 KB |
| httpd.conf | 7/8/2021 7:37 PM | CONF File | 1 KB |
| index.html | 7/8/2021 7:37 PM | Firefox HTML Doc... | 2 KB |
| initrun.sh | 7/8/2021 7:38 PM | SH File | 1 KB |
| jpeg-arm | 7/8/2021 7:37 PM | File | 8 KB |
| passwd | 7/10/2021 9:41 AM | File | 1 KB |
| ppsapp | 7/8/2021 8:00 PM | File | 2,659 KB |
| ppsFactoryTool.txt | 7/8/2021 7:46 PM | TXT File | 1 KB |
| ppsMmcTool.txt | 7/8/2021 7:38 PM | TXT File | 1 KB |
| set | 7/8/2021 7:37 PM | File | 1 KB |
| upload.html | 7/8/2021 7:37 PM | Firefox HTML Doc... | 1 KB |



Creator mode ☐

ROM file: ppsapp

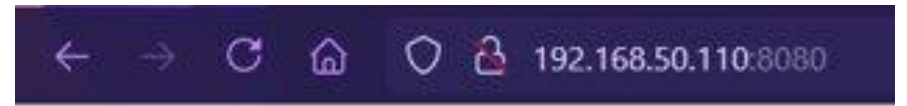
CRC32: a221d69c

MD5: e5e559715d01cf8060d56ba97ce4a79c

SHA-1: 49c5541efce351fdc81818595ceccd2272627892

Patch file: ppsapp-onvif.zip

6. Command and Control



[System Volume Information/](#)
[bin/](#)
[busybox](#)
[cgi-bin/](#)
[env](#)
[etc/](#)
[hack](#)

```
> telnet 192.168.50.110 23
```

```
BusyBox v1.20.2 (2020-12-05 17:05:42 CST) built-in shell (ash)  
Enter 'help' for a list of built-in commands.
```

```
/ # /mnt/mmc01/busybox whoami  
root  
/ #
```

7. Actions on Objective

← → ↺ 🏠 🛡️ 🔒 192.168.50.110:8080/cgi-bin/

./
../
[cleanup.cgi](#)
[main.cgi](#)
[mjpeg.cgi](#)
[snap.cgi](#)

← → ↺ 🏠 🛡️ 🔒 192.168.50.110:8080/cgi-bin/snap.cgi ☆ 🧑 🌟 ⬇️ ⌚ >>



Open Media

File Disc **Network** Capture Device

Network Protocol

Please enter a network URL:

rtsp://admin:admin@192.168.50.110:8554/Streaming/Channels/101

http://www.example.com/stream.avi
rtp://@:1234
mms://mms.examples.com/stream.asx
rtsp://server.example.org:8080/test.sdp

rtsp://192.168.50.110:8554/Streaming/Channels/101 - VLC media player

Media Playback Audio Video Subtitle Tools View Help

07-10 13:08:14

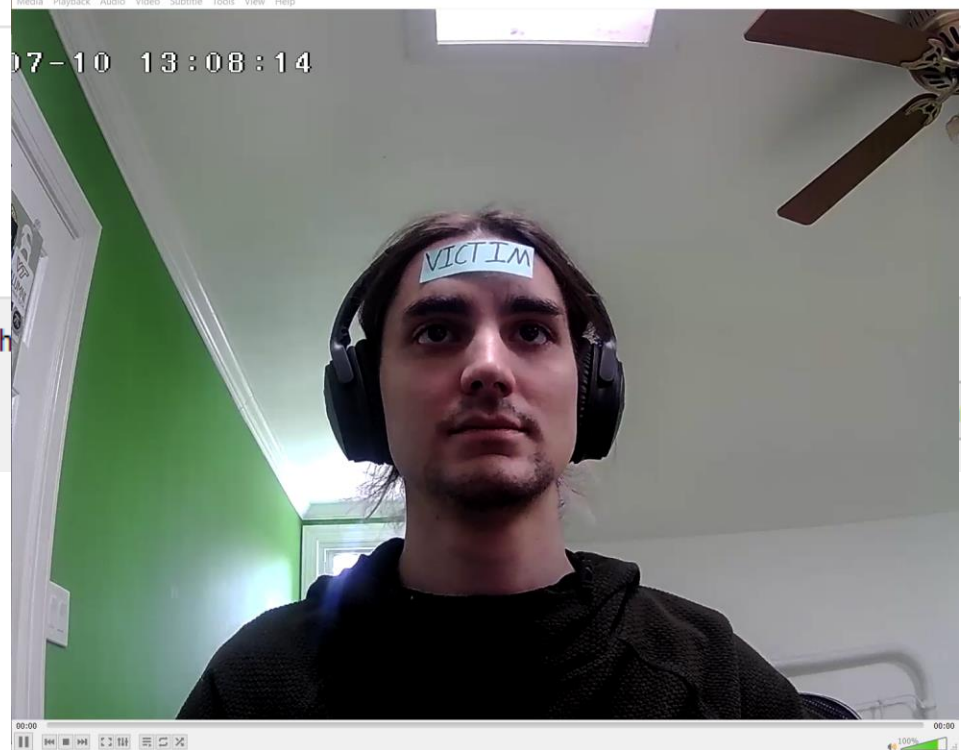
☐ Show playlist

Cancel

00:00 00:00

⏮ ⏪ ⏩ ⏭ 🔍 ⏴ ⏵ ⏸ ⏹

100%





Yellow Belt Home Security

Consumer Mitigation Tips:

Low Difficulty

- Google search your chosen device(s) and stay aware
- Previously owned smart devices
- Factory reset
- Reduce physical access
- Change the device defaults as permitted
- Just don't buy

Blue Belt Home Security

Medium Difficulty:

- Two factor authentication
- Change default network name

```
    } else {
      break;
    }
  }

  for (const startParent of startNodeAndParents.parentNodes) {
    if (
      startParent.type !== "Program" &&
      startParent.type !== "File" &&
      util.locEnd(startParent) <= util.locEnd(endNodeAndParents.node)
    ) {
      resultStartNode = startParent;
    } else {
      break;
    }
  }

  return {
    startNode: resultStartNode,
    endNode: resultEndNode
  };
}

addAlignmentSize = addAlignmentSize || 0;

const result = parser.parse(text, opts);
const ast = result.ast;
text = result.text;

const formattedRangeOnly = formatRange(text, opts, ast);
if (formattedRangeOnly) {
  return { formatted: formattedRangeOnly };
}

let cursorOffset;
if (opts.cursorOffset >= 0) {
  const cursorNodeAndParents = findNodeAtOffset(ast, opts.cursorOffset);
  const cursorNode = cursorNodeAndParents.node;
  if (cursorNode) {
    cursorOffset = opts.cursorOffset - util.locStart(cursorNode);
    opts.cursorNode = cursorNode;
  }
}

const astComments = attachComments(text, ast, opts);
const doc = printAstToDoc(ast, opts, addAlignmentSize);
opts.newLine = guessLineEnding(text);
const toStringResult = printDocToString(doc, opts);
let str = toStringResult.formatted;
if (hasUnicodeBOM) {
  str = String.fromCharCode(UTF8BOM) + str;
}
const cursorOffsetResult = toStringResult.cursor;
#ensureAllCommentsPrinted(astComments);
```



Black Belt Home Security

High Difficulty:

- Whitelisting/allowing only needed device protocols
- Segment IoT devices
- Device software/firmware updates





Session Terminated

- Conclusions
- Access to our project files
 - GitHub:

The background of the slide features a person wearing a dark hoodie, holding a laptop. The person is positioned in the center-right of the frame. The background is a dark blue or black, filled with a dense, vertical stream of green binary code (0s and 1s) that appears to be falling or scrolling, reminiscent of the 'Matrix' effect. A large, semi-transparent white circle is overlaid on the left side of the image, containing the title and list of references.

References

- <https://github.com/guino/Merkury1080P>
- <https://www.logsign.com/blog/7-steps-of-cyber-kill-chain/>
- <https://owasp.org/www-project-internet-of-things/#tab=IoT> Attack Surface Areas
- <https://blogs.juniper.net/en-us/security/secondhand-iot-devices-firsthand-threats-to-security>