2020 年国内外典型物联网安全事件盘点

2021 年 1 月

青莲云物联网安全研究院收集整理

前 言

物联网技术正在加速向各行业渗透，根据中国信通院《物联网白皮书（2020 年）》内容显示：预计到 2025 年，物联网连接数的大部分增长来自产业市场，产业物联网的连接数将占到总体的 61.2%。智慧工业、智慧城市 、智慧交通、智慧健康、智慧能源等领域将最有可能成为产业物联网连接数增长最快的领域。

当业界在推动产业物联网高速发展同时，物联网安全问题也给我们敲响了警钟。2020 年，国内外挖矿、设备劫持事件频发，智能家居产品不断爆出安全漏洞，漏洞被利用时将造成不可逆的经济损失，同时也反映在物联网产业建设初期，安全作为物联网应用的基础设施的重要性。

青莲云物联网安全研究院整理了 2020 年国内外物联网安全事件，希望设备厂商、项目设计方、实施监理方等能够更加重视物联网安全，在

项目初期建设环节引入物联网安全解决方案，尽量减少不必要的安全风险。

青莲云安全点评

1) 物联网僵尸网络非常活跃，不同的病毒变种版本持续发起无差别攻击，恶意行为以 DDoS 和挖矿为主
2) 国家关键基础设施成为物联网攻击的重要目标
3) 各国相继出台了有关物联网安全的法律、指南及安全合规要求
4) 与物联网业务相关的基础平台，如云主机、APP、中间件成为黑客攻击的新目标
5) 传统企业在开展物联网智慧化转型的过程中更容易受到黑客攻击，原因在与前期缺乏物联网安全架构设计

一月

物联网供应商 Wyze 确认服务器发生泄露

http://hackernews.cc/archives/29091

伪装为 WAV 的恶意软件在受害设备上挖矿 但其 bug 导致 BSOD

http://hackernews.cc/archives/29339

研究发现五家美国电信企业易受 SIM 卡交换攻击

http://hackernews.cc/archives/29282

VPN 警告：REvil 勒索软件盯上未打补丁的 Pulse Secure VPN 服务器

http://hackernews.cc/archives/29142

儿童信息安全不容忽视！别让智能产品变成罪犯帮凶

http://www.youxia.org/2020/01/49777.html

三菱电机遭网络攻击

https://www.solidot.org/story?sid=63311

黑客泄露 51 万服务器路由器的 Telnet 密码

https://www.solidot.org/story?sid=63305

二月

车联网安全系列——特斯拉 iBeacon 隐私泄露

https://www.anquanke.com/post/id/197750

境外黑客组织未攻击我国视频监控系统，但确给我们敲响了警钟

https://www.secfree.com/17021.html

三月

俄罗斯联邦安全局被爆雇佣外包商启动物联网 DDoS 攻击项目 Fronton

http://hackernews.cc/archives/29714

调查发现医院很多设备采用过时操作系统 易受黑客攻击

http://hackernews.cc/archives/29672

Android 安全警告：10 亿台设备不再获得更新

http://hackernews.cc/archives/29654

警惕 Linux 挖矿木马 SystemMiner 通过 SSH 爆破入侵攻击

http://hackernews.cc/archives/29619

台湾合勤和利凌物联网设备漏洞正被利用

https://www.solidot.org/story?sid=63903

加密漏洞允许黑客克隆丰田现代起亚的汽车遥控钥匙

https://www.solidot.org/story?sid=63750

黑客劫持路由器 DNS：以 COVID-19 之名重定向至恶意网站

http://hackernews.cc/archives/29803

四月

史上最强大的僵尸网络 Dark_nexus 横空出世

https://www.secrss.com/articles/18506

到 2024 年，物联网连接总数将达到 830 亿，不断增长的网络引发了新的安全问题

https://www.helpnetsecurity.com/2020/04/02/total-iot-connections/

黑客利用雷克萨斯和丰田汽车漏洞发起远程网络攻击

https://www.easyaq.com/news/2147307724.shtml

五月

伊朗港口被网络攻击，居然是来自以色列的报复？

https://www.secrss.com/articles/19621

奔驰智能汽车组件 OLU 源码泄露

https://www.4hou.com/posts/Qvkq

新型 Kaiji 恶意软件通过 SSH 暴力攻击针对物联网设备

https://www.easyaq.com/news/2147307804.shtml

六月

趁火打劫 | 恶意攻击者的魔爪正伸向医疗物联网

https://www.4hou.com/posts/g6kD

Windows 10 Version 2004 新 BUG：重复报告安全警报

http://hackernews.cc/archives/31290

GuardMiner 挖矿木马近期活跃，具备蠕虫化主动攻击能力，已有较多企业中招

http://hackernews.cc/archives/31248

英特尔处理器又曝两个 SGX 新漏洞 攻击者可轻松提取敏感数据

http://hackernews.cc/archives/31070

央视曝光 APP 偷窥乱象，“隐私记录功能”或将在手机操作系统中推广

http://www.youxia.org/2020/06/52161.html

每天有 80000 台打印机通过 IPP 在线曝光

https://www.freebuf.com/news/241211.html

七月

饱受折磨的家用路由器 | 在研究的 127 个家用路由器中，没有一个路由器幸免

https://www.4hou.com/posts/x9zB

以色列供水设施上个月又遭到两次网络攻击

https://www.secrss.com/articles/24040

注意！多款智能家居 Hub 存在远程代码执行漏洞

https://www.4hou.com/posts/0OD5

Pwn2Own Tokyo ：Netgear R6700 路由器堆溢出漏洞分析

https://www.4hou.com/posts/8OKj

八月

Tor 被曝多个 0 day 漏洞，官方给出回应！

https://www.4hou.com/posts/n8VW

九月

智能咖啡机被发现很容易修改

https://www.solidot.org/story?sid=65670

物联网设备存在较大安全隐患 专家可轻松掌控 Smarter 咖啡机

http://hackernews.cc/archives/32334

数十亿设备面临 BLESA 低功耗蓝牙重连欺骗攻击的安全威胁

http://hackernews.cc/archives/32176

十月

Linux 5.9.1 以及部分旧版稳定内核已解决 “Bleeding Tooth”漏洞问题

http://hackernews.cc/archives/32653

安全研究人员演示如何通过入侵广告牌来误导特斯拉 Autopilot 发生碰撞

http://hackernews.cc/archives/32567

监狱视频探视服务 HomeWAV 暴露了囚犯与律师之间的私下通话

http://hackernews.cc/archives/32468

研究人员警告 T2 芯片存在无法修复的漏洞 导致 Mac 设备易受攻击

http://hackernews.cc/archives/32420

物联网僵尸网络被用于充当代理服务器

https://www.solidot.org/story?sid=65847

腾讯主机安全（云镜）捕获 WatchBogMiner 挖矿木马新变种，利用 Apache Flink 漏洞攻击云主机

http://hackernews.cc/archives/33019

腾讯：无感支付充电桩存严重安全漏洞，有“盗刷”隐患

https://cloud.tencent.com/developer/news/712977

十一月

Windows 勒索软件被发现移植到 Linux 平台

https://www.solidot.org/story?sid=66032

特斯拉 Model X 遭遇黑客中继攻击 3 分钟可开走汽车

http://hackernews.cc/archives/33609

首个 HomePod 越狱事件引发对智能音箱黑客潜力的猜测

http://hackernews.cc/archives/33580

ZeroLogon 已被黑客组织大量用于全球范围内的工业攻击

http://hackernews.cc/archives/33538

十二月

黑客打开了莫斯科 2732 个包裹储物柜：成千上万只包裹面临被盗风险

https://mp.weixin.qq.com/s/CSirUTzD4KLnfoa6904LZg

研究称通用电气医疗成像设备中的硬编码密码或使患者数据面临风险

http://hackernews.cc/archives/33976

谷歌黑客详细介绍了利用零点击“Wormable”Wi-Fi 入侵 iPhone 的方法

http://hackernews.cc/archives/33839

黑客组织利用黑匣子攻击技术从意大利 ATM 机中盗走了 80 万欧元

http://hackernews.cc/archives/33754

FBI 警告：黑客正在劫持低安全性的智能设备

http://hackernews.cc/archives/34465

以上报告由青莲云物联网安全研究院收集整理，如果您的企业有任何物联网安全问题或物联网安全建设需求，欢迎与青莲云取得联系，我们将第一时间为您提供详细的安全咨询服务。