

Understanding the Internet of Things

July 2020

Understanding the Internet of Things

Benefits of the IoT

This interconnectedness has brought about immense benefits to consumers in terms of productivity, convenience, time and cost savings, and a greater quality of life.

These benefits are a result of 3 key factors enabled by IoT:



Remote Monitoring

Users can access data and information easily, remotely, and in real time, reducing the need to make physical trips.



Automation and Control

With Machine-to-Machine (M2M) communication, devices can stay connected and manage everyday tasks without the need for human intervention.



Predictive Analysis

With IoT, users can know things in advance. E.g. In healthcare, smart sensors analyse health conditions and lifestyle choices and recommend preventative measures to reduce disease occurrences.

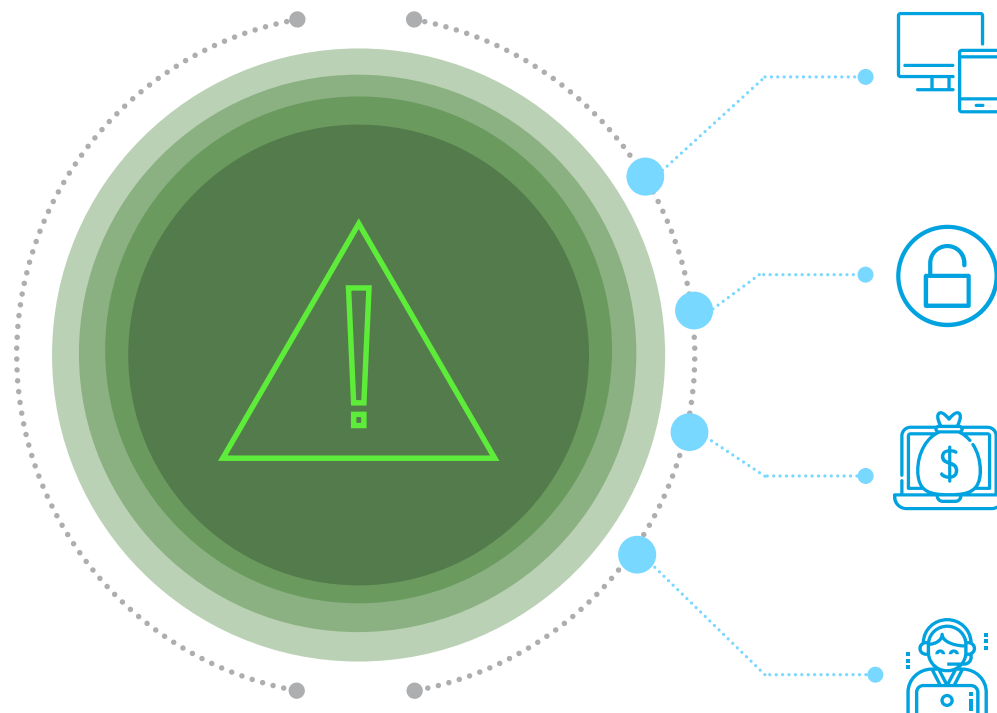
<https://www.linkedin.com/pulse/advantages-disadvantages-internet-things-iot-tommy-quek/>
<https://www.iotforall.com/iot-healthcare-advantages-disadvantages/>

Understanding the Internet of Things

Security challenges in the IoT

According to a forecast by Business Insider, there will be over 64 billion IoT devices by 2025. Despite these trends, there are still a few key IoT security challenges to be addressed in order for us to fully harness the potential of IoT.

Challenges for the future of IoT:



Outdated hardware and software

A majority of IoT devices either do not get the appropriate updates, or never get a single one. This means the products become vulnerable to attacks when hackers find bugs or security issues.

Use of weak and default credentials

Many IoT companies sell devices and provide default credentials with them which are easy to find and often used by hackers to carry out brute-force attacks to compromise these devices and use them for nefarious purposes.

Malware and ransomware

The rapid rise of IoT products makes cyberattack permutations unpredictable. Cybercriminals have been able to lock consumers out of their own IoT devices.

Data security and privacy

With increased interconnectedness, data protection has become more difficult as it gets transferred between multiple devices within a few seconds, which can lead to a data leak.

<https://readwrite.com/2019/09/05/9-main-security-challenges-for-the-future-of-the-internet-of-things-iot/>
<https://www.peerbits.com/blog/biggest-iot-security-challenges.html>

Understanding the Internet of Things

Case Study: Mirai malware

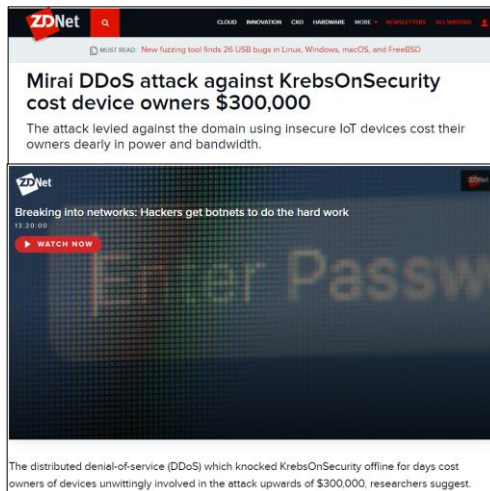
One of the most well-known IoT attacks is the Mirai malware, which targets online consumer devices such as IP cameras and home routers.

First discovered in August 2016, the Mirai malware has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks, including:

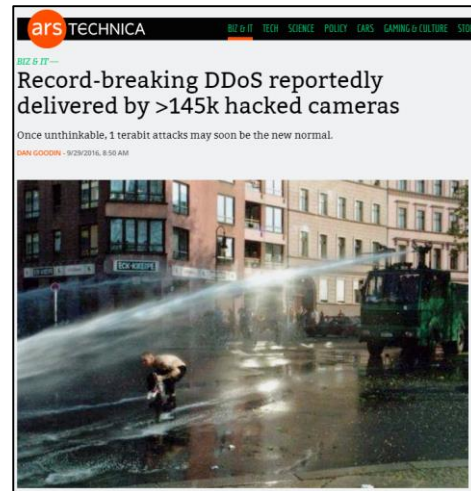
- Krebs on Security – A blog specialising in cyber-crime
- OVH – One of the largest European hosting providers
- DYN – A popular DNS provider in US

Devices infected by Mirai continuously scan the internet for vulnerable IoT devices and logs into them using a table of more than 60 common factory default usernames and passwords to infect them.

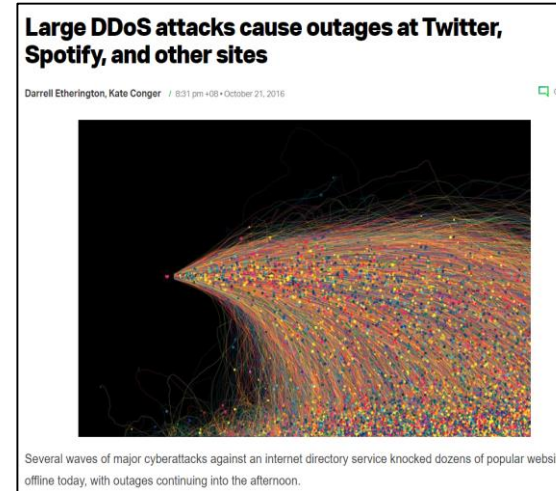
These attacks exceeded 1 Tbps – one of the largest on public record – and infected over 600,000 vulnerable IoT devices.



Read more: [ZDNet](#)



Read more: [Ars Technica](#)



Read more: [TechCrunch](#)

<https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/>

Understanding the Internet of Things

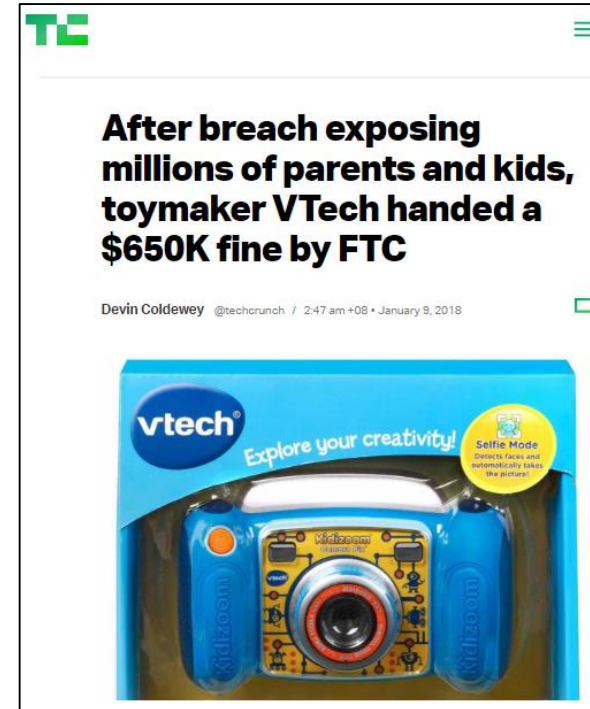
Case Study: VTech smart toys

VTech, the maker of “smart” toys such as watches and cameras, was fined US\$650,000 for exposing data from millions of parents and children due to poor security practices.

A security researcher found that profiles of parents and children set up on VTech, which included pictures and personal details, could be accessed via one of the company’s websites.

Furthermore, not only was the website not secure, the data were not encrypted in transit or at rest, contradicting security claims made in VTech’s privacy policy.

As a result of VTech’s poor security practices, at least 5 million parent records and 227,000 child records were shown to be accessible.



Read more: [Tech Crunch](#)

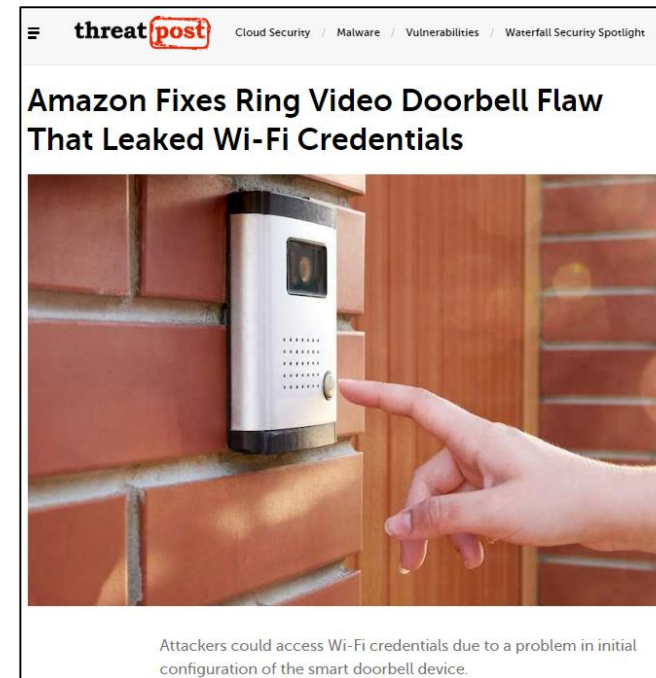
Understanding the Internet of Things

Case Study: Ring smart doorbell

Ring smart doorbell is a popular home security device acquired by Amazon.

In February 2019, researchers found that Ring contains a serious flaw that could allow an attacker on a shared WiFi network to spy on families' video and audio footage.

In November 2019, researchers discovered yet another vulnerability in Ring that could allow attackers to access the owner's Wi-Fi network credentials and potentially reconfigure the device to launch an attack on the home network.



Read more: [Threat Post](#)

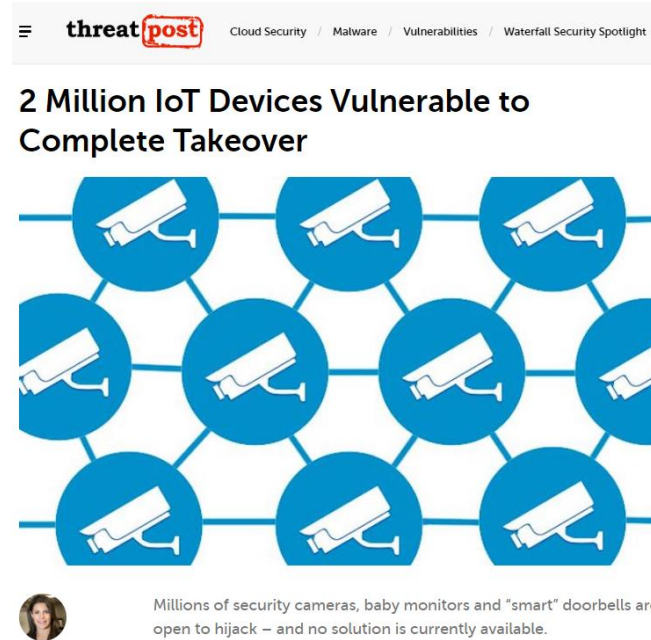
Understanding the Internet of Things

Case Study: iLnp2P

Over 2 million devices using an iLnp2P component – including IP security cameras, baby monitors and smart doorbells – have serious vulnerabilities.

In April 2019, security engineer Paul Marrapese discovered two vulnerabilities in a P2P solution, iLnp2P, that could allow remote hackers to find and take over vulnerable cameras used in the devices.

In other words, an attacker can hijack the devices and spy on their owners. There is still no known patch for these security flaws.



The image is a screenshot of a Threat Post article. At the top, the Threat Post logo is visible, along with navigation links for 'Cloud Security', 'Malware', 'Vulnerabilities', and 'Waterfall Security Spotlight'. The main headline reads '2 Million IoT Devices Vulnerable to Complete Takeover'. Below the headline is a graphic consisting of a grid of blue circles, each containing a white icon of a security camera. The circles are interconnected by thin lines, suggesting a network. Below the graphic is a small circular profile picture of a woman and a text block that reads: 'Millions of security cameras, baby monitors and "smart" doorbells are open to hijack – and no solution is currently available.'

Read more: [Threat Post](#)

Understanding the Internet of Things

Ways to protect your IoT devices

IoT can bring a lot of convenience to our lives and to guard against potential threats, it is very important to secure your the IoT devices in your smart home to prevent cyber attacks.

Here are some ways to help secure your smart home:

01

Change default usernames and passwords.

Cybercriminals probably already know the default passwords that come with many IoT products. Choose devices that allow you to change the default password.

02

Use strong, unique passwords for Wi-Fi networks and device accounts.

Use unique, complex passwords made up of letters, numbers, and symbols. Use a strong encryption method (such as WPA2) when you set up Wi-Fi network access to keep your network secure.

03

Disable features you may not need.

IoT devices come with a variety of services such as remote access, often enabled by default. If you do not need it, be sure to disable it.

04

Keep your software up to date.

Do not put off installing software updates, as it might be a patch for a security flaw.

05

Use two-factor authentication.

Two-factor authentication (2FA) — such as a one-time code sent to your mobile phone — can keep hackers out of your accounts. If your smart-device apps offers 2FA, use it.

06

Set up a guest network.

Keep your Wi-Fi account private. Visitors, friends and relatives can log into a separate network that does not tie into your IoT devices.

07

Ensure physical security.

Ensure that IoT devices are kept in a secure location where attackers cannot simply walk up and tamper with them. If the device supports tampering alarms such as CCTV cameras, enable this feature.



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax & legal and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organisation”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 312,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

About Deloitte Singapore

In Singapore, services are provided by Deloitte & Touche LLP and its subsidiaries and affiliates.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.