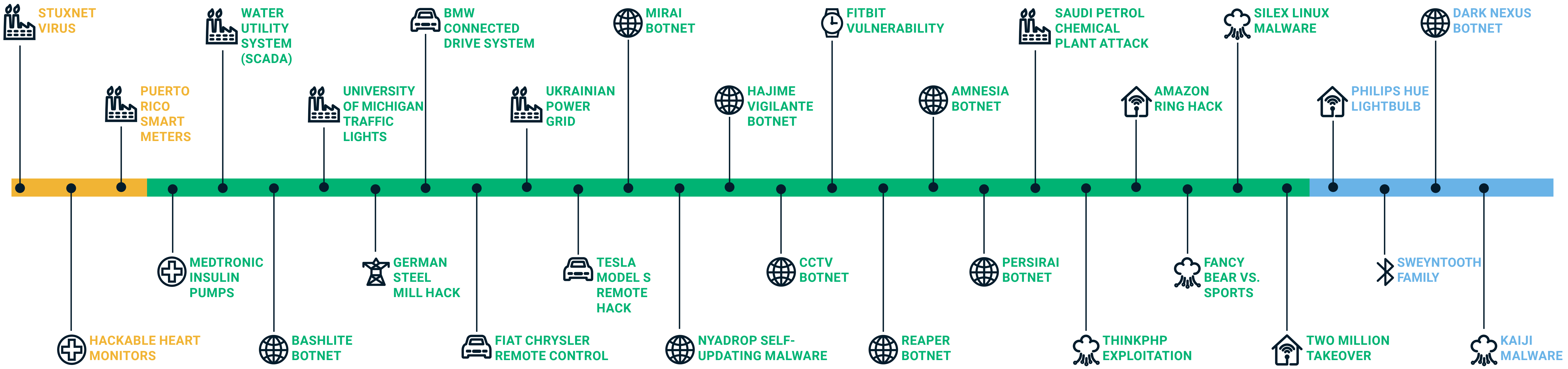
Evolution of IoT Attacks

SECTIGO

By 2025, there will be 41.6 billion connected IoT devices, generating 79 zettabytes (ZB) of data (IDC). Every Internet-connected "thing," from power grids to smart doorbells, is at risk of attack.

Throughout the last few decades, cyberattacks against IoT devices have become more sophisticated, more common, and unfortunately, much more effective. However, the technology sector has fought back, developing and implementing new security technologies to prevent and protect against cyberattacks. This infographic shows how the industry has evolved with new technologies, protocols, and processes to raise the bar on cybersecurity.

- BLUETOOTH
- BOTNET
- CAR
- INDUSTRIAL
- GENERIC IOT
- INFRASTRUCTURE
- MEDICAL
- SMART HOME
- WATCH/WEARABLE



First Era | THE AGE OF EXPLORATION | 2005 - 2009

Security is not a priority for early IoT/embedded devices. Most cyberattacks are limited to malware and viruses impacting Windows-based embedded control systems. Instead of actively putting up a defense, organizations simply assume no one would bother to attack these devices running in isolated networks. Security methods and technologies include:

- Security by obscurity
- Minimal security, often easily bypassed
- Secure protocols (SSH or SSL) used in a few systems, usually no other security controls
- Air-gapped networks

Second Era | THE AGE OF EXPLOITATION | 2011 - 2019

The number of connected devices is exploding, and cloud connectivity is becoming commonplace. With the continued acceleration of attacks targeting IoT devices, criminals improve their ability to monetize these attacks through crypto mining, ad-click fraud, and spam email campaigns. Nation-state attackers exploit IoT devices for political motivated attacks. Companies are beginning to address security for IoT devices, but the level of protection is inconsistent, and many connected devices still have significant secure flaws.

While many new security technologies are being adopted, their use is inconsistent, incomplete, and sometimes flawed, resulting in many devices that remain vulnerable. Security technologies used for some IoT and embedded devices include:

- Security protocols (TLS and SSH)
- Secure boot
- TPM or Secure Element for secure key storage
- Hardened operating system
- Embedded Firewall

Third Era | THE AGE OF PROTECTION | 2020

Connected devices are ubiquitous in every area of life, from transportation and manufacturing to medicine and entertainment. In response to this growing number and severity of attacks, governments and industrial groups begin to enact legislation requiring higher levels of security for IoT devices.

Because hackers will continue to find "soft targets" in legacy and new devices implemented without strong security measures, companies worldwide are beginning to build strong security controls into IoT devices, using security frameworks and unified solutions with key security technologies that work together to provide multiple layers of protection. Chief components of these frameworks include:

- Security protocols (TLS and SSH)
- Secure boot
- TPM or secure element for secure key storage
- Hardened operating system
- Embedded firewall and intrusion detection
- Data at rest protection
- Certificates/PKI for authentication and identification

First Era

THE AGE OF EXPLORATION

STUXNET VIRUS 2005

Risk: Operational disruption
Used to attack a uranium enrichment facility at Natanz, Iran, this virus was an early indicator of IoT vulnerabilities and how they can lead to critical national infrastructure breaches.

HACKABLE HEART MONITORS 2008

Risk: Safety
Researchers found that implantable cardiac defibrillators (ICDs) could be externally controlled, allowing intruders to intercept medical information and manipulate the device by taking advantage of the unencrypted signals in the ICD's built-in radio.

PUERTO RICO SMART METERS 2009

Risk: Operational disruption

An electrical utility in Puerto Rico was estimated to have lost hundreds of millions of dollars after the power consumption figure was manipulated, allowing the smart meters to be controlled by external devices and not accurately measure the amount of power used.

Second Era

THE AGE OF EXPLOITATION

MEDTRONIC INSULIN PUMPS 2011

Risk: Safety
Software and a special antenna allowed researchers to locate and seize control of any device within 300ft through its radio transmitters, potentially making it pump excessive quantities of insulin into the blood.

WATER UTILITY SYSTEM (SCADA) 2011

Risk: Operational disruption
Hackers destroyed a water pipe outside the city of Illinois by gaining access to the industrial control system. They were able to burn out one of the utility's pumps by causing the SCADA system that controlled it to turn the pump on and off repeatedly.

BASHLITE BOTNET 2014

Risk: Denial of service
BASHLITE infected more than 2M devices in two years. Spreading through brute-forcing, BASHLITE was able to launch several types of large-scale DDoS attacks simultaneously. A 2020 version could also deploy cryptocurrency-mining and bricking malware.

UNIVERSITY OF MICHIGAN TRAFFIC LIGHTS 2014

Risk: Safety
Researchers seized control of an entire system of over 100 intersections from a single access point. Easily hacked, the traffic light system used wireless radios for its communication infrastructure with very basic encryption and no password.

GERMAN STEEL MILL HACK 2014

Risk: Operational disruption
Hackers used spear phishing to infiltrate a German steel mill's network and manipulate its controls to compromise a multitude of systems, including industrial components on the production network and a blast furnace which could not be properly shut down, resulting in substantial damage.

BMW CONNECTED DRIVE SYSTEM 2015

Risk: Financial
Researchers exploited a vulnerability in BMW's Connected Drive system and imitated BMW servers to send remote unlocking instructions to vehicles. The test took advantage of the remote unlocking feature, which could be requested via a BMW assistance line.

FIAT CHRYSLER REMOTE CONTROL 2015

Risk: Safety
Uconnect, a smart feature which controls the Fiat Chrysler vehicles' entertainment and navigation, was found to have a vulnerability that opened the chip in the car's head unit to malicious code, which in turn could be used to send commands to manipulate physical components including steering and brakes.

UKRAINIAN POWER GRID 2015

Risk: Operational disruption
Hackers compromised the internal corporate network through spear-phishing malware emails. They were then able to seize control of the SCADA network and turn substations off, leaving 230K people without electricity. The malware also disabled IoT control devices by implanting malicious firmware on the devices.

TESLA MODEL S REMOTE HACK 2016

Risk: Safety
Researchers remotely hacked an unmodified Tesla Model S and took over the multimedia system and dashboard displays, switched on the turning signals, and unlocked the doors without using a key. They also managed to activate the windshield wipers, fold in the side mirror, and open the trunk – all while the car was moving.

MIRAI BOTNET 2016

Risk: Denial of Service
The infamous IoT botnet Mirai took advantage of IoT devices with weak or default passwords and gained control of large numbers of compromised closed-circuit TV cameras and routers, using them to launch a DDoS attack that crippled large swathes of the internet including Twitter, the Guardian, Netflix, Reddit, and CNN. The source code was then released into the wild.

NYADROP SELF-UPDATING MALWARE 2016

Risk: Denial of Service
This brute-force attack targeted IoT devices by running through a vast list of common usernames and passwords until it gained access. Once in, NyaDrop dropped other malware onto the victim device. It was difficult to diagnose and remove because it would self-delete and alter its malware each time it successfully hacked into a system.

HAJIME VIGILANTE BOTNET 2016

Risk: Operational disruption
More sophisticated than Mirai, Hajime would fight rival botnets for control of a device. Hajime had no tools for DoS attacks, only ways to continue expanding its reach and keep fighting other botnets. It is known for leaving quirky messages on compromised systems, such as "Stay sharp!"

CCTV BOTNET 2016

Risk: Denial of Service
This botnet hijacked 25.5K internet-connected CCTV cameras to conduct network attacks against online shops. The massive operation was able to regularly flood websites with 35K HTTP requests per second. This could escalate into a tsunami of 50K HTTP requests per second if defensive measures were not taken.

SECTIGO

FITBIT VULNERABILITY 2017

Risk: Data loss
Researchers found that some Fitbit products were vulnerable to intrusions and that messages transmitted between fitness trackers and cloud servers could be intercepted. Once inside the internal network, hackers could manipulate and share data with third parties.

REAPER BOTNET 2017

Risk: Denial of Service
An evolution of Mirai, the Reaper botnet is believed to have infected up to 1M devices, making it the largest IoT botnet in history. It took control of embedded devices, infecting cameras, routers, storage boxes, and more. Reaper is especially dangerous because its code can be easily updated to launch subsequent attacks via queued botnets.

AMNESIA BOTNET 2017

Risk: Denial of Service
This botnet targeted an unpatched remote code execution flaw in DVR devices, affecting approximately 227K devices, gaining full control and allowing attackers to launch broad, Mirai-sized DDoS attacks on targets globally.

PERSIRAI BOTNET 2017

Risk: Denial of Service
Following Mirai's steps, Persirai downloaded DDoS software onto internet-enabled cameras and infected more than 120K devices across a thousand different camera brands and models.

SAUDI PETROL CHEMICAL PLANT ATTACK 2018

Risk: Operational disruption
Attackers gained remote access to an engineering workstation by deploying malware which reprogrammed SIS controllers. It then managed to trigger an explosion which caused physical damage to the plant's infrastructure.

THINKPHP EXPLOITATION 2018

Risk: Denial of Service
Attackers leveraged CVE-2018-20062, a remote code execution (RCE) vulnerability in Chinese open source PHP framework ThinkPHP, to implant a variety of malware which was used to spread cryptocurrency miners. While primarily targeting web servers, a large number of IoT devices were also infected.

AMAZON RING HACK 2019

Risk: Safety
A hacker was able to watch and communicate with an 8-year-old girl in Mississippi by hacking an Amazon Ring camera her parents had installed in her bedroom, using a password found in an online database of previously compromised login information.

FANCY BEAR VS. SPORTS 2019

Risk: Operational disruption
Fancy Bear, the Russian-sponsored hacker group, conducted significant cyberattacks on 16 national and international sports and anti-doping organizations. In a number of these attacks, IoT devices were utilized as a point of ingress.

SILEX LINUX MALWARE 2019

Risk: Operational disruption
The hacker used a new strain of malware to brick up to 4K insecure IoT devices running on the Linux or Unix operating systems that had known or guessable default passwords. The malware would trash devices' storage, remove firewalls and network configuration, and ultimately "brick" them, causing them to not be able to boot.

TWO MILLION TAKEOVER 2019

Risk: Safety
Researchers revealed that two million security cameras, baby monitors, and smart doorbells could be used to spy on their owner without any manual configuration—and there is no known patch for the discovered flaw. The attack method is traced back to two vulnerabilities in the peer-to-peer technology solution iLnkP2P developed by Shenzhen Yunni technology.

Third Era

THE AGE OF PROTECTION

PHILIPS HUE LIGHTBULB 2020

Risk: Denial of Service
Researchers showed how a single smart light bulb can infect an entire network by seizing control and loading it with malware, which forced it to misbehave.

SWEYNTOOTH FAMILY 2020

Risk: Denial of Service
Researchers spotted a family of 12 vulnerabilities in BLE software development kits belonging to six major system-on-a-chip vendors. The vulnerabilities allowed intruders within radio range to trigger crashes, deadlocks, buffer overflows, and even bypass security.

DARK NEXUS BOTNET 2020

Risk: Denial of Service
Rapidly developing with over 40 versions in three months, Dark Nexus comprises over 1.3K bots. Its source code reuses components from BASHLITE and Mirai, but this botnet can also disguise the malicious traffic it throws at the target as legitimate web browser traffic.

KAIJI MALWARE 2020

Risk: Denial of Service
Researchers discovered a malware strain specifically built to infect IoT devices and Linux-based servers. The Kaiji botnet is coded from scratch and executes brute-force attacks through SSH ports exposed on the internet. While the initially discovered version of the malware seems incomplete, researchers are closely monitoring its development.

SECTIGO