Evolution of IoT Attacks: *An Interactive Infographic*

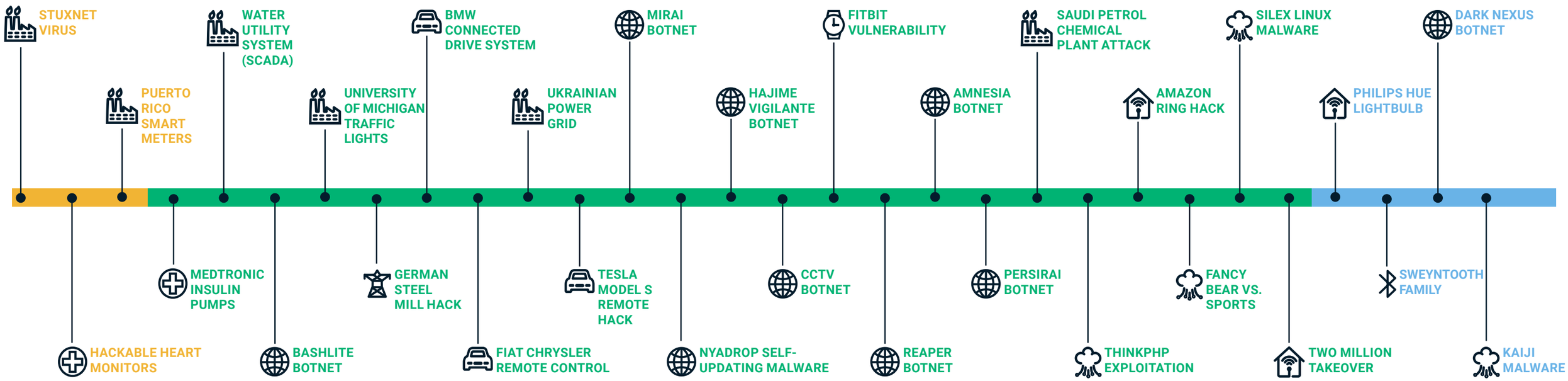
SECTIGO

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

Throughout recent decades, cyberattacks against IoT devices have become more sophisticated, more common, and unfortunately, much more effective. However, the industry has fought back, developing and implementing new security technologies to prevent and protect against attacks. 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

Mouse over each attack for more information.



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 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. Criminals improve their ability to monetize attacks on IoT devices through crypto mining, ad-click fraud, and spam email campaigns. Nation-state actors use IoT devices for politically motivated attacks. While many new security technologies are being adopted, their use is inconsistent, incomplete, and sometimes flawed, resulting in many devices that are still vulnerable:

- 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 began 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 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