THE 2023 IOT SECURITY LANDSCAPE REPORT

Bitdefender | NETGEAR

WWW.BITDEFENDER.COM/IOT

FOREWORD

In 1950, science fiction author Ray Bradbury wrote of what is now known as a “smart home.” Set in the year 2026 after a nuclear war, his short story *There Will Come Soft Rains* tells of a house that keeps up its daily routines even though it’s the only standing structure in an abandoned city.

In terms of realism, Bradbury missed the mark somewhat with his description of a helpful house going about a perfect routine even in the absence of humans. A more accurate novel could have told a story of millions of tiny devices and sensors enrolled in botnets dealing devastating DDoS attacks, home video surveillance cameras manipulated by distant criminals, and baby monitors turned into the ears of creepy strangers lurking on the Internet.

THEY DON'T MAKE CONSUMER ELECTRONICS LIKE THEY USED TO

The Internet of Things (IoT) is a network of devices, vehicles, home appliances and other items that use sensors, software and network connectivity to collect and exchange data. These devices are changing the way we live, work and communicate. They are also opening up new avenues for crime, as IoT devices are among the most vulnerable equipment in the world.

As manufacturers increasingly scrap "dumb" devices in favor of Internet-connected versions, smart homes are growing around their owners, enveloping the humans that own them without them even knowing it. The once romanticized notions of the smart house of yore, often portrayed on TV as a cheery aide to a seamless life, have given way to privacy invasions, data breaches and ruthless ransomware attacks targeting network attached storage. If improperly configured, or if shipped with vulnerabilities and security hazards that were overlooked during quality assurance, these devices can spell catastrophe for privacy and data integrity, or even jeopardize the integrity of the Internet itself.

Since 2014, Bitdefender has been building cybersecurity technologies to help protect the modern smart home. These technologies are built into the router to monitor traffic going to and from the Internet, protecting the devices on the network and eliminating the efforts and costs associated with multiple security subscriptions or software.

KEY FINDINGS

This report is based on threat intelligence sampled by **2.6 million smart homes** around the world protected by NETGEAR Armor powered by Bitdefender. We investigated about **120 million IoT devices** generating a whopping **3.6 billion security events** around the world to uncover vulnerabilities and attack scenarios and make the smart home a safer environment for everybody.

2.6 Million households

Sending 3.6 billion security events and helping paint a clearer picture of what the smart home looks like in 2023

46 Devices per household

US homes have an average of 46 devices connected to the Internet. European households have an average of 25 devices

8 Attacks every 24h

Home networks see an average of 8 attacks against devices every 24 hours

UNDERSTANDING THE SMART HOME

A look at the most popular devices and the top vulnerabilities affecting them

5

Bitdefender | NETGEAR

APRIL 25, 2023

COMPUTERS

Computers and laptops are a frequent encounter in connected homes. While they have lost to mobile devices in popularity, they still witness a steady growth worldwide.

STREAMING DEVICES

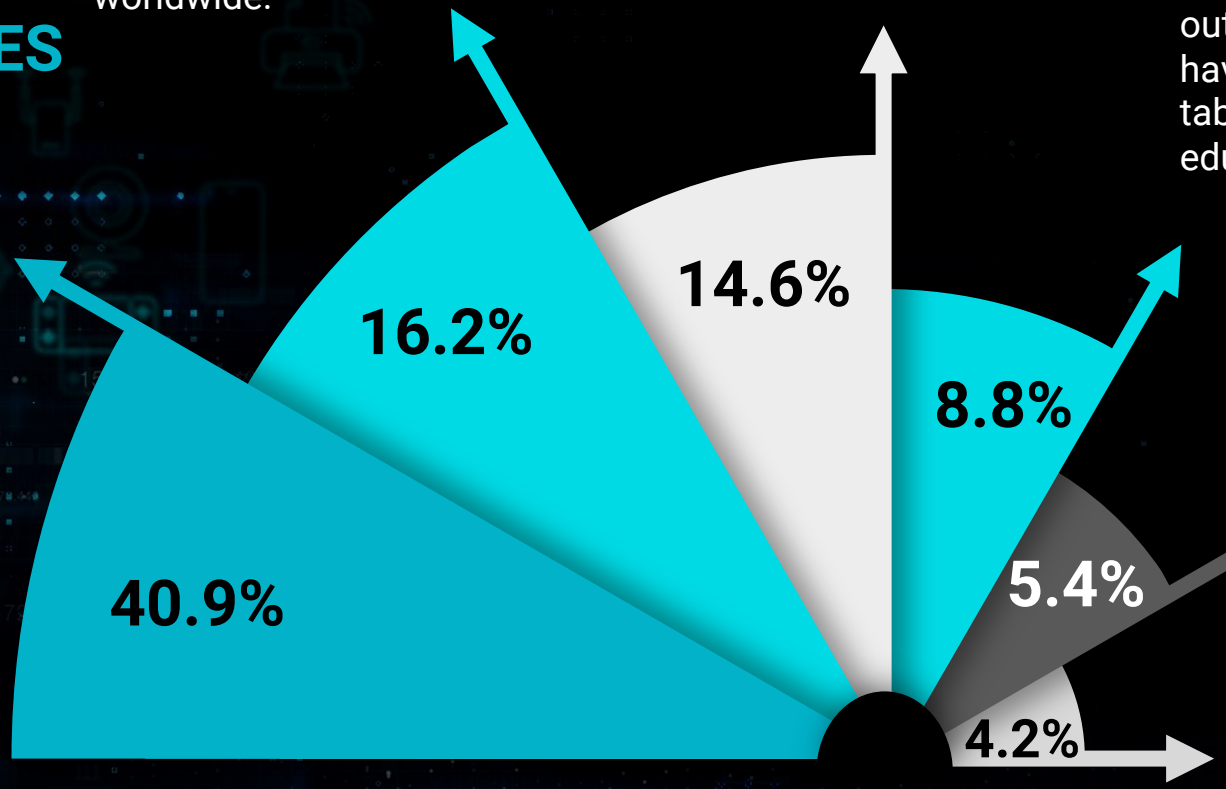
Streaming devices are popular means of turning a “dumb” TV into an Internet-connected device.

TABLET

Tablets have gained significant traction during the COVID-19 outbreak as schools have started issuing tablets for online education.

SMARTPHONES

Almost 41% of the devices connected to home routers are smartphones. This number includes guest devices that can be temporarily associated with the network.



SMART TV

Smart TVs may only account for 5.4% of internet-connected devices, but they are among the most vulnerable IoT devices in the smart home.

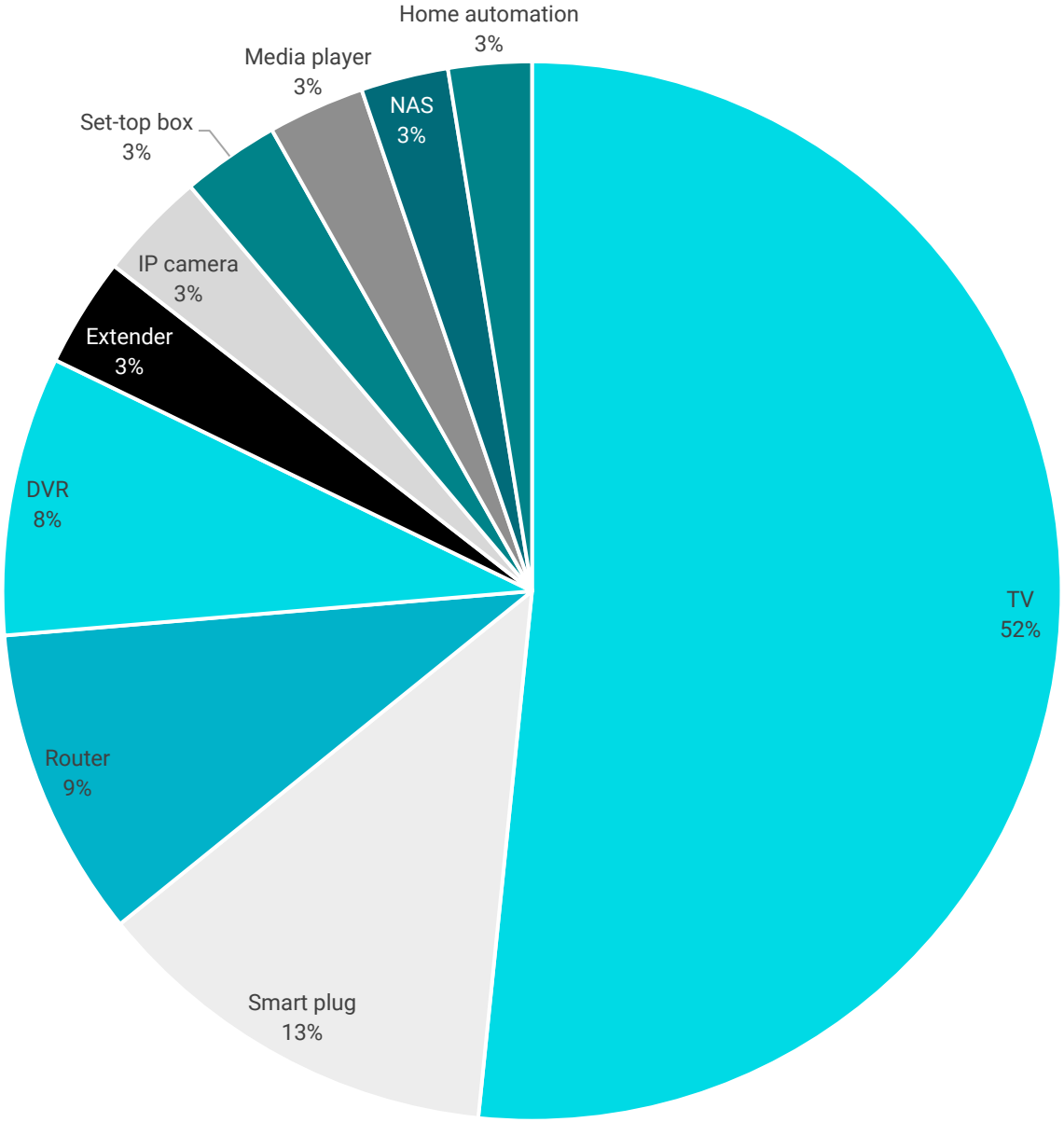
CONSOLE

Game consoles also double as entertainment centers.They come with dedicated hardware and software for playing games, and typically connect to a TV or monitor to display the game.

MOST VULNERABLE IOT DEVICES IN 2022

Smart TVs are leading the top of most vulnerable devices, although they are not among the most popular devices in users' homes. Over half of IoT vulnerabilities identified by Bitdefender affect smart TVs.

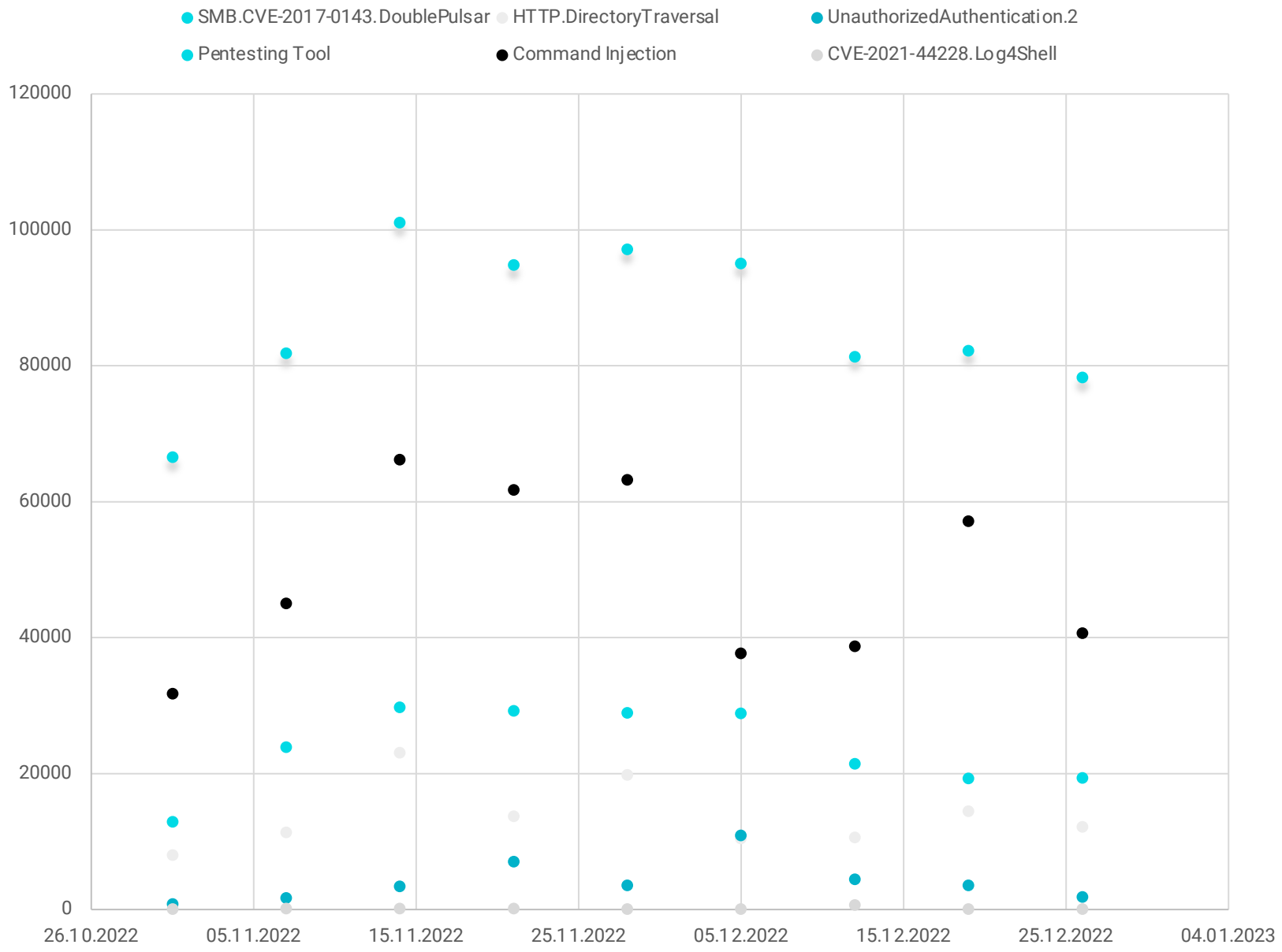
Smart plugs have also become increasingly popular during 2022 as more and more consumers are relying on monitoring energy usage to face the rising energy costs.



IOT ATTACKS BLOCKED BY ARMOR™

Exploitation of IoT devices such as Smart TVs and Smart Plugs targets different outcomes, depending on device type and attacking botnet capabilities.

Most of the attacks spotted in 2022 rely on already known common vulnerabilities and exposures (CVEs) that are included in automated attack toolkits. Although these vulnerabilities are known to both IoT vendors and attackers, it may take significant time for firmware vendors to assess, patch and deliver fixes for the devices already deployed in smart homes potentially giving cybercriminals a window of opportunity.



Bitdefender | NETGEAR

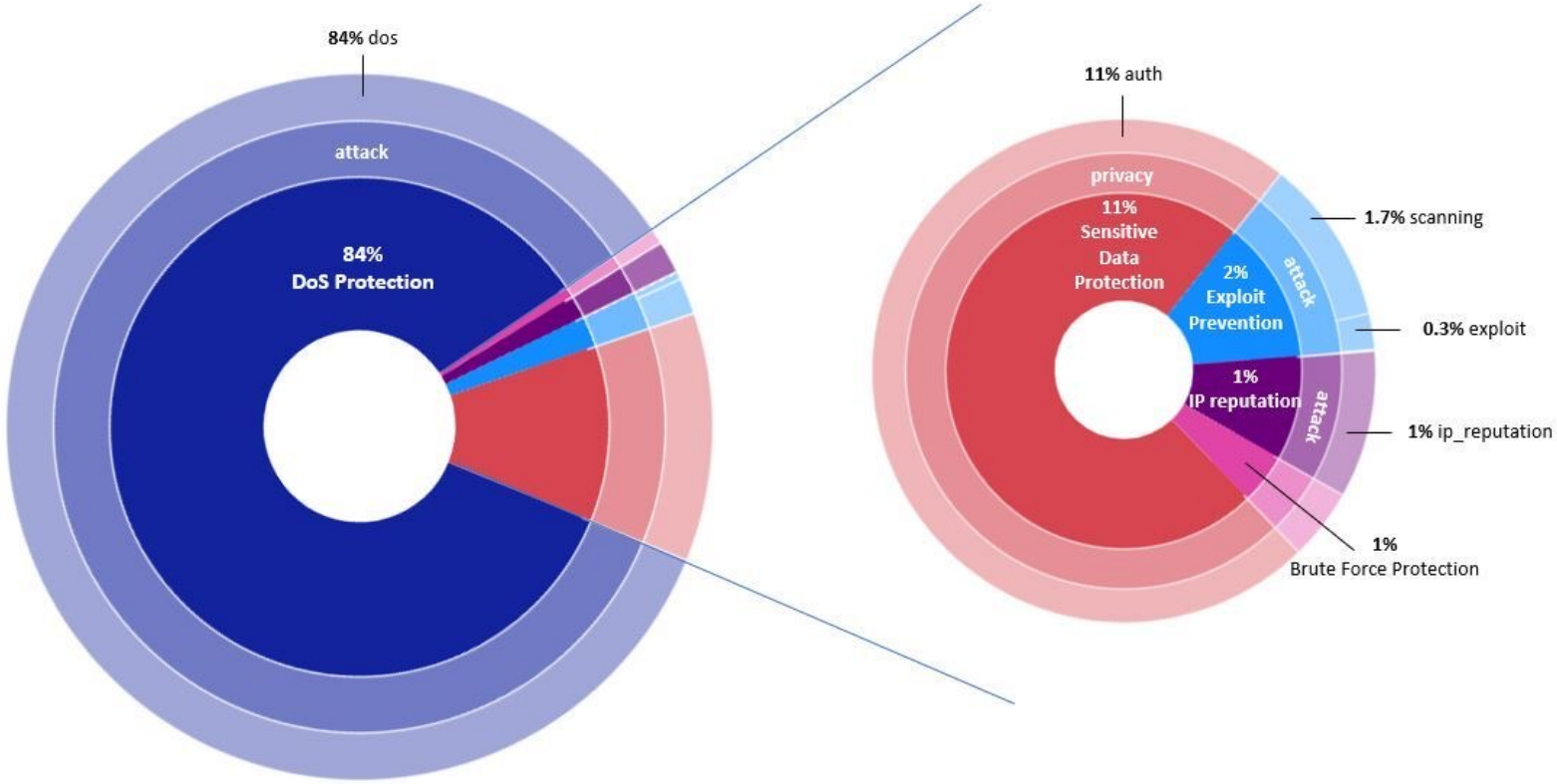
APRIL 25, 2023

VULNERABILITIES BY PROTECTION TECHNOLOGY

Blocking these attacks calls for layered technologies to stop them cold before they reach the vulnerable IoT device in your network.

Key to Bitdefender's detection capabilities are the Behavior Protection, Network Attack Defense and IP Reputation technologies.

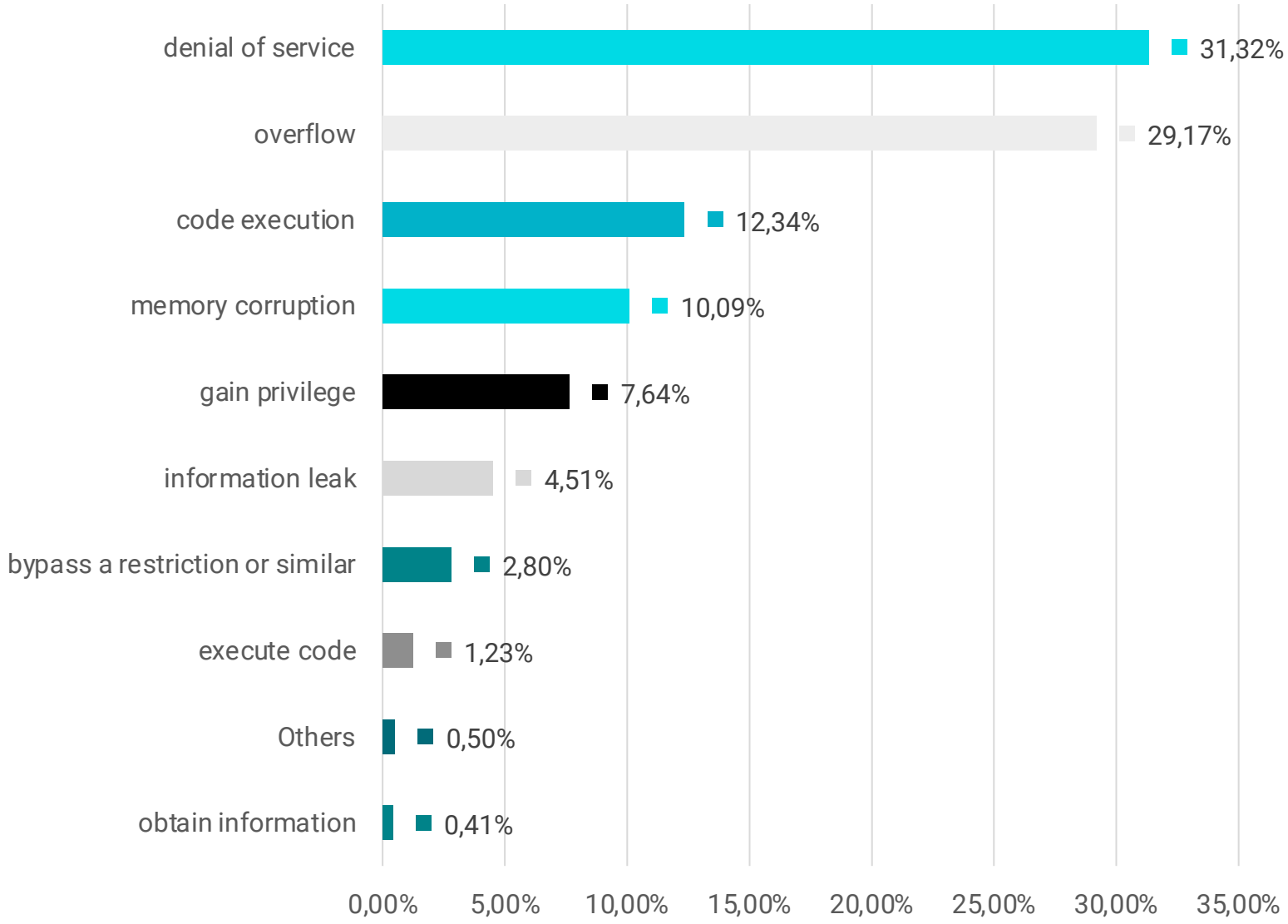
Denial of Service remains the number one attack type with over 84% of all incidents recorded in 2022. Eleven percent of all recorded incidents target sensitive data, while device exploitation accounts for 2% of all analyzed reports.



VULNERABILITIES BY TARGETED OUTCOME

Exploitation of IoT devices targets different outcomes, depending on device type and purpose, connectivity options and monetization opportunities.

Vulnerability outcomes range from undermining the systems' capacity to perform expected functions to executing code on the device and hijacking its functions.



IOT RISKS TO CONSIDER

CYBERSECURITY RISKS

Smart homes are vulnerable to cyberattacks, as many IoT devices have weak security measures. This can allow hackers to gain access to personal information, such as passwords and financial data, and even take control of the smart devices.

PRIVACY CONCERNS

Many smart devices are equipped with cameras, microphones, and other sensors that can collect data about users without their knowledge or consent. This can result in violation of privacy, which is be particularly concerning for in-house deployment.

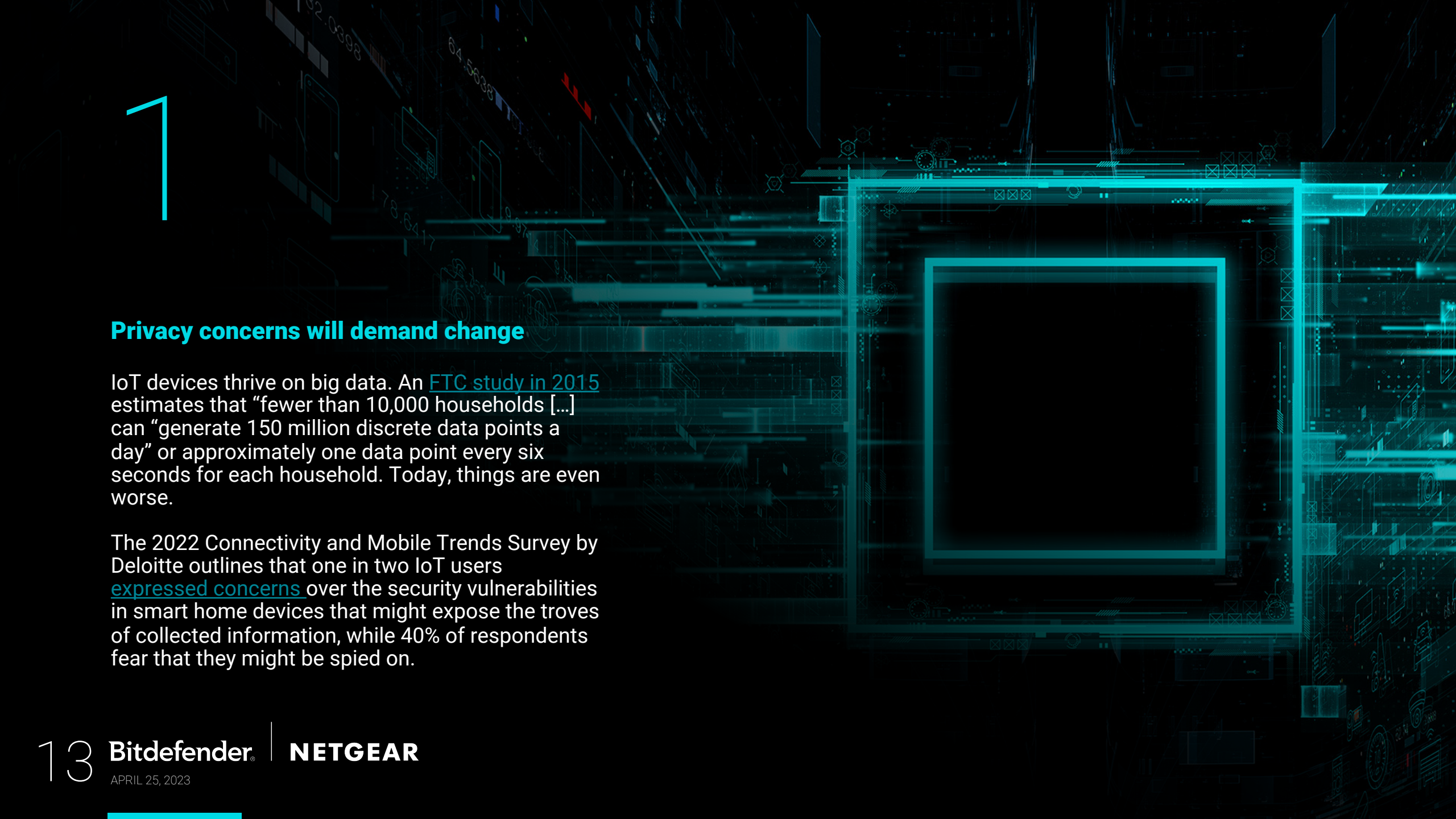
PHYSICAL SAFETY RISKS

Smart plugs, door locks and cameras are becoming increasingly popular. These devices control physical security aspects such as lighting, access control and surveillance. Any disruption in operation or loss of control can impact on physical security.

PREDICTIONS FOR 2023

12 Bitdefender | NETGEAR

APRIL 25, 2023



1

Privacy concerns will demand change

IoT devices thrive on big data. An FTC study in 2015 estimates that "fewer than 10,000 households [...] can "generate 150 million discrete data points a day" or approximately one data point every six seconds for each household. Today, things are even worse.

The 2022 Connectivity and Mobile Trends Survey by Deloitte outlines that one in two IoT users expressed concerns over the security vulnerabilities in smart home devices that might expose the troves of collected information, while 40% of respondents fear that they might be spied on.

2

Botnets will continue to grow

IoT devices will increasingly become targets for botnets, which can launch large-scale distributed denial-of-service (DDoS) attacks. Cyber-criminals will continue to invest significant efforts in exploitation and persistence mechanisms to help them grow their infected device base.

3

IoT security will get worse before it gets better

Vendors' slow reaction to vulnerability disclosure and patching will persist into 2023. Although new regulations - such as the EU Cyber Resilience Act - are anticipated to provide some relief by imposing mandatory cybersecurity standards for products sold within the bloc, their enforcement is not expected until at least 2025.

HOW CAN USERS STAY SAFE

- Both home users and employees should be aware of active IoT devices in their networks and keep them up to date. If some devices are past their end of life, replace them with newer models.
- Move all smart devices to a dedicated guest network to isolate them from the main network
- Patch devices as soon as a new firmware version becomes available.
- Use routers or gateways with built-in security.
- Probe the home network for vulnerable devices with a smart home scanner
- Avoid exposing LAN devices to the Internet unless necessary

This report is based on cyber-security insights received between January 1 and Dec 31, 2022.

ROUTER SECURITY

As crucial Internet infrastructure, routers are exposed to a wide range of security threats. A combination of outdated software, lack of encryption, weak passwords, misconfigured remote management, as well as an overall lack of on-device security mechanisms allows attackers to hijack routers and enroll them into botnets, get into the network and gain control of the connected devices.

Now with NETGEAR Armor powered by Bitdefender, home users have access to advanced cybersecurity on Orbi mesh WiFi systems and Nighthawk routers.

NETGEAR Armor combines NETGEAR's long-standing pursuit to deliver the fastest & latest connectivity with Bitdefender's award-winning technology to secure all connected devices in every home.


Bitdefender®
WWW.BITDEFENDER.COM/IOT