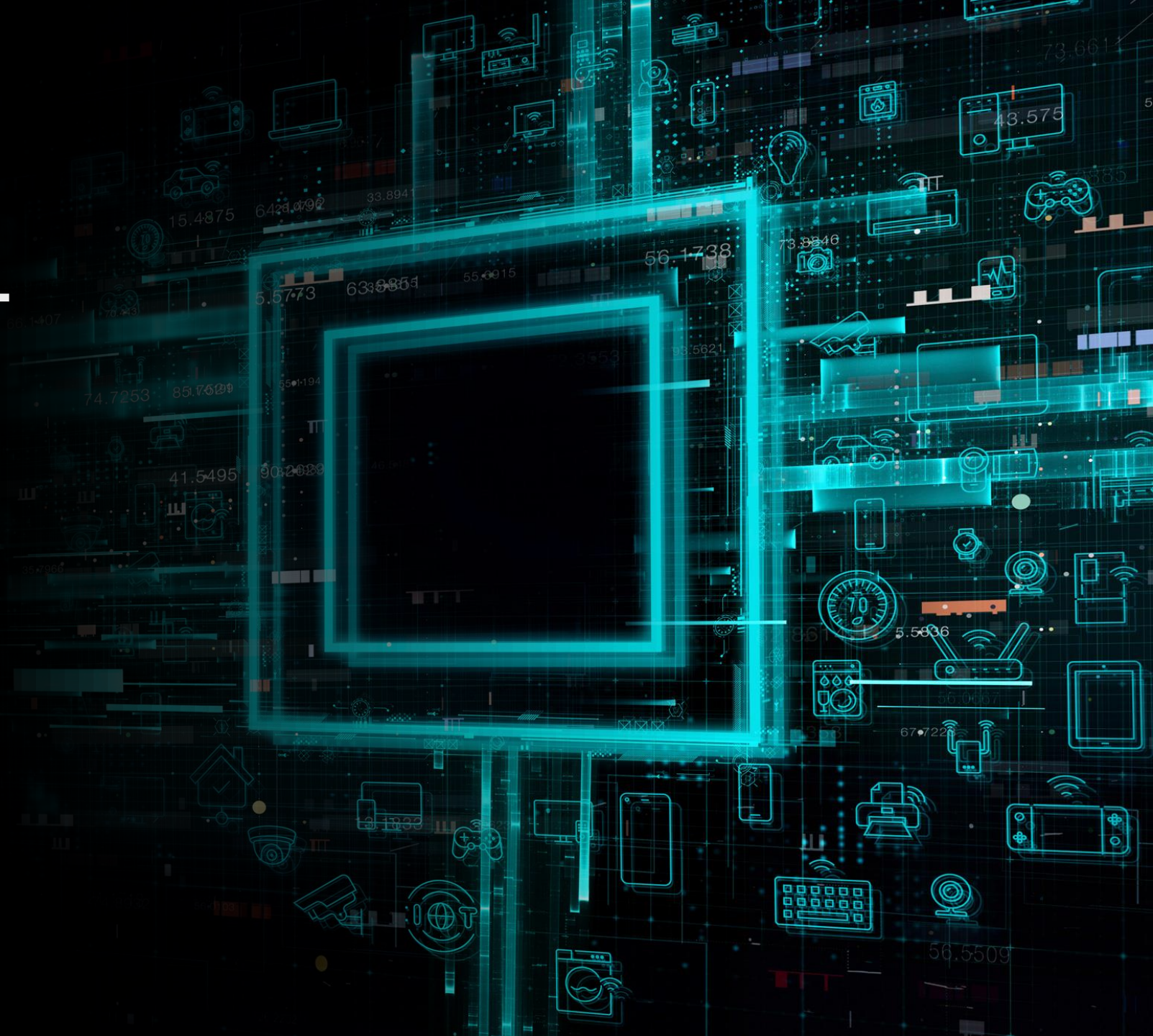
THE 2026 IOT SECURITY LANDSCAPE REPORT



Bitdefender | NETGEAR

WWW.BITDEFENDER.COM/IOT

ABOUT THIS REPORT

This report is built on Bitdefender and NETGEAR security events sampled between January and September 2026 — 9 months of automated observation across roughly 10.4 million routers protected by Bitdefender smart-home security technologies.

Across that window, the sensors logged 5.4 billion security events and 6.2 billion vulnerability observations against devices sitting behind those routers. We also placed these insights next to the year's better- documented public IoT incidents - in Slovakia, Iran and inside smart- TV app stores - to ask a broader question.

That question is no longer only *can this device be hacked?* It is: what can this device see, what network position does it occupy, and what can an adversary do with the trust, bandwidth or sensors attached to it.

What counts as an event: *An event is a detection record: a port scan stopped at the router, a brute-force login attempt, an exploit pattern matched and blocked. It is not proof of compromise. Most of what we count is automated machinery probing everything that answers.*

What counts as a vulnerability observation: *Devices behind protected routers are identified and matched against known-vulnerability data. One observation is one device–vulnerability pairing; a single device can generate many such pairs.*

THE CONNECTED WORLD NEVER SLEEPS

The 2025 edition of this report described an internet that never stops knocking. In 2026 the knocking got louder — and the house behind the door got more interesting. Four numbers open this year's account.

10.4 million households

Sharing information on more than 5 billion attack attempts on routers and connected devices

24 devices per household

The average household has 24 connected devices

90% is port scanning

4.85 billion of the 5.4 billion attack-category events were automated port scans.

5.4 billion vulnerabilities

This report is based on analysis of about 5.4 billion vulnerabilities exploitation attempts against live IoT targets

NOTABLE IOT INCIDENTS IN 2026

YOUR TELEVISION MAY HAVE A SECOND JOB

In July 2026, security firm Spur described a quiet industry running inside consumer smart-TV apps. SDKs bundled with free apps on several app stores open a local proxy listener on the television. The household's broadband connection then carries third-party traffic — the marketed workloads are AI web-scraping, ad verification and market research, not classic criminal botnets.

None of this is malware as documented. Users accept consent language when the app is installed; providers present the product as consented infrastructure, and - per the original reporting - traffic flows only after that consent. The question the reporting raises is whether a one-time EULA click on a free app is informed consent for turning a television into a third party's exit node.

A television relaying third-party traffic shares its IP reputation with everything it relays - scraping runs, ad-fraud probes, account checks - and the household owns the address the outside world sees.

RESIDENTIAL PROXY

A relay service that routes customer traffic through ordinary household IP addresses instead of data centers, making automated traffic look like everyday users. The "exit node" is the device whose address the outside world sees. Televisions are prized as exits: always on, rarely watched for traffic, and trusted by reputation systems .

“WE OWN THE GLASS”

The Gamers Nexus team reports that LG TVs may gather far more than viewing data: **voice recordings**, **details of other devices on the local network**, **geographical location** and **nearby wireless networks** — with their reporting indicating that collection may continues when the TV **appears to be off, or is disconnected from the local network**. According to their reporting, underneath sits **Automatic Content Recognition (ACR)**, which identifies what is on screen irrespective of app or service and feeds personalized marketing.

According to the same reporting, LG’s advertising materials pitch campaigns that extend **from the TV to other devices in the household** — and footage cited by Gamers Nexus shows three separate LG executives saying “we own the glass” or “we own the TV” on camera. Gamers Nexus estimates that roughly **216,000,000** devices may exhibit this behavior. Bitdefender has not independently verified this estimate.

This is a **consent** story, not a hack. The unresolved question is whether changes buried in TV terms and privacy policies constitute informed agreement to whole-home sensing - and Gamers Nexus warns the pattern “isn’t just an LG problem,” expecting other manufacturers to behave much the same. Either way the living-room display has become a sensor-plus-advertising endpoint: the same device class that, in our own telemetry, accounts for **22.7% of all vulnerability observations** - the largest single share - and where LG-branded labels alone carry **197.4 million** CVE observations, 16.6% of the rollup. These counts reflect the prevalence of these devices in our dataset and are no a ranking of any manufacturer’s security practices.

AUTOMATIC CONTENT RECOGNITION

Software that continuously samples the pixels (and sometimes audio) to identify content being viewed, played, or displayed. It typically works by creating a digital “fingerprint” of the content and matching it against a reference database.

WHEN THE SENSOR IS PART OF THE STREET

In August 2026, Slovakia's National Security Authority (NBÚ) issued an advisory on **NERO R-ONE** road-enforcement devices - Chinese-origin hardware imported by an European reseller and allegedly procured with EU funds.

Analysis of delivered units uncovered an undocumented remote-access path through the devices' cellular module: an **SMS-triggered remote shell**, **hardcoded credentials for an unauthenticated root account** on the FTP/web interface, a default module password permitting FTP and HTTP access, and **Secure Boot disabled** in the configuration supplied to Slovakia.

Scale:

- **861 units** planned nationwide under the modernization program;
- **279 delivered and analyzed** at the time of assessment; the advisory itself references
- **~13,000 similar mobile cameras** in use across EU member states. NBÚ - with the Interior Ministry, SK-CERT and the intelligence services - coordinated the review and recommended the devices **not be connected to operational networks** until remediated. Government services warned the devices "could be exploited to surveil critical infrastructure, record traffic, or be activated en masse."

WHAT A CAMERA NETWORK REVEALS WHEN CONTROL CHANGES HANDS

In February 2026, a joint US–Israeli strike killed Iran's Supreme Leader, Ayatollah Ali Khamenei, near his Pasteur Street compound in Tehran. Three days later, the Financial Times published how the timing had been set: every traffic camera in Tehran had reportedly been hacked for years, and their feeds had quietly built what intelligence sources called a "pattern of life" around the leadership.

The mechanics read like a targeting handbook written against municipal infrastructure. Planners reportedly used one camera near where bodyguards parked their cars to reconstruct schedules, routes and guard assignments, then ran the accumulating footage through algorithms that assembled files on individual officials.

On the morning of the strike, roughly a dozen mobile-phone towers around Pasteur Street were jammed so bodyguard calls would go unanswered.

"We knew Tehran like we know Jerusalem, " one official told the paper.

The cameras were one stream among hundreds, per the reporting - signals intelligence, human sources and social network analysis all fed the same picture, and much of the detail remains classified. What is documented is the cameras' role: not the decision-maker, but the persistent, well-placed sensor that made everyone else's information timely.

IOT IS NO LONGER JUST A TARGET

ROLE 01

TARGET

The conventional model. Devices are **scanned, brute-forced, exploited or knocked offline** - 90.1% of what our sensors saw this year was exactly this, repeating every day against 10.4 million home networks.

ROLE 02

PROXY

The device's **identity and bandwidth** have value. Residential IPs relay third-party traffic - via criminal botnets like BADBOX, malware-free SDKs inside TV apps, or both - because a household address inherits trust a data center never gets.

ROLE 03

SENSOR

The device **sees or hears the physical world**: TVs sample screens and rooms, cameras read streets. The value is the observation - sold onward as ad data, or collected, in Tehran's telling, as targeting intelligence.

ROLE 04

FOOTHOLD / INFRASTRUCTURE

The device **occupies a persistent trusted position** - the router everything flows through, the NAS holding the family archive, the enforcement camera wired into municipal systems. Whoever holds that position holds everything behind it.

SMART HOME TRENDS IN 2026

What 6.2 billion vulnerability observations and 5.4 billion attack events say about the connected household - measured, this time, at router scale.

THE SMART HOME

Fingerprinting plus vulnerability matching turns every observed household into a ranked list of device-CVE records. Read in aggregate, 6.2 billion CVE observations sketch the shape of the modern connected home: dominated not by exotic “IoT gadgets” but by the mainstream furniture of the network - the television, the plug on the wall, the storage box in the corner.

20%

MOBILE PHONES

The connected home’s control hub, bringing communication, entertainment and access to smart devices together on one screen.

11%

TV

Large screens with their own apps and internet connections, adding another layer of connected software to the living room.

10%

COMPUTER

These devices connect home networks to sensitive files, personal accounts and corporate resources.

6%

STREAMING DEVICE

Dedicated gateways to online entertainment, bringing streaming services to home screens

53%

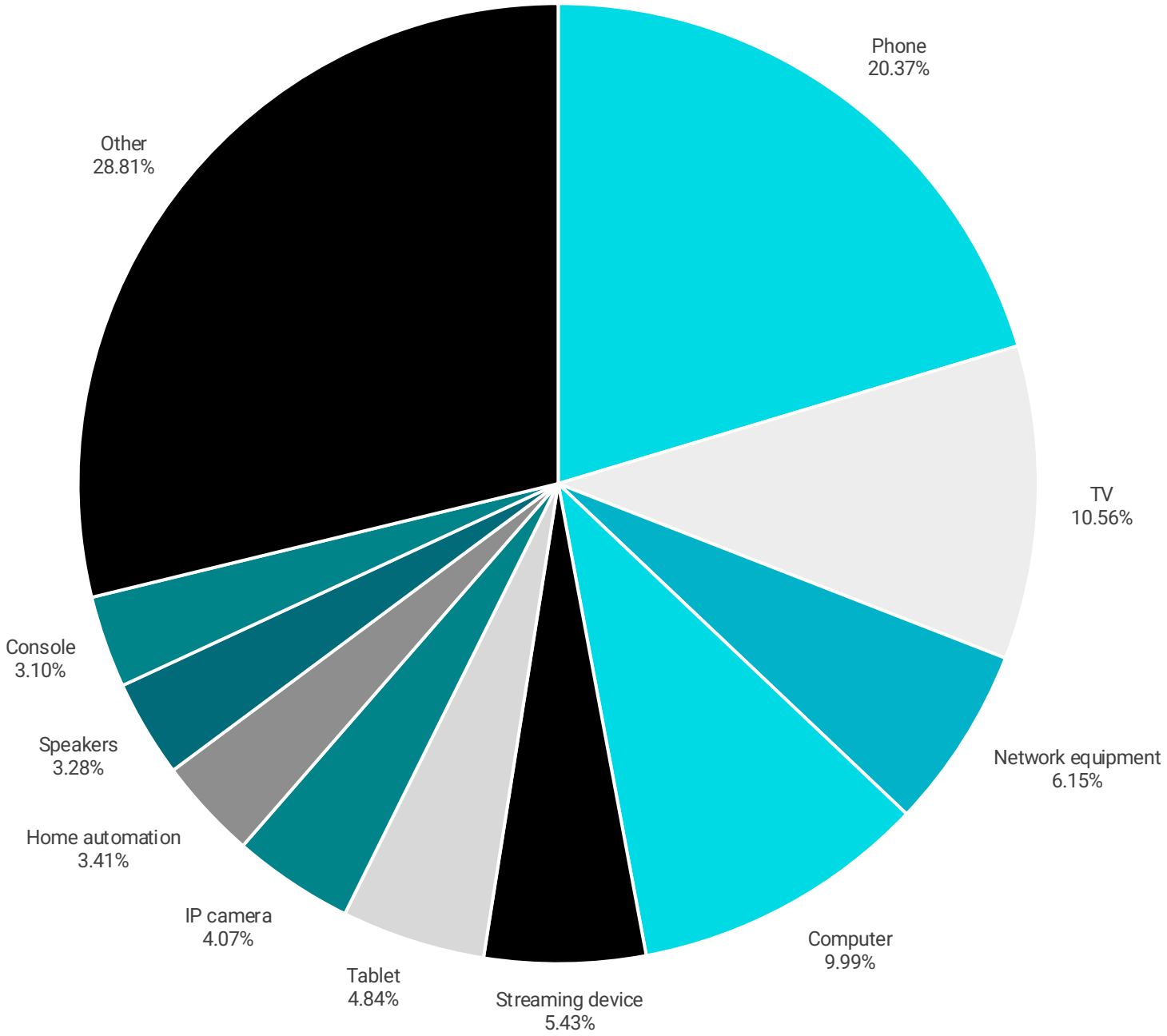
EVERYTHING ELSE

From network equipment to smart appliances, the remaining devices reveal how far household connectivity extends beyond familiar screens.

THE SMART HOME BUILDING BLOCKS

Phones remain the most common identified devices in the connected home, accounting for 20.4% of the mix. TVs follow at 10.6%, ahead of computers at 10.0% and streaming devices at 5.4%. Together with speakers and consoles, TVs and streaming devices represent 22.4% of connected equipment, highlighting entertainment's substantial footprint on the household network.

Network equipment accounts for 6.2%, while tablets contribute 4.8%. IP cameras and home automation devices add another 7.5%, extending connectivity into monitoring and household control. "Other" remains the largest category at 28.8%, with a very diverse mix of devices. The result is a household network spanning personal computing, entertainment and physical infrastructure, with protection needed across the full mix.



THE INTERNET KEEPS KNOCKING

A home router keeps a full calendar of unsolicited attention. Across our protected households, the first 9 months of 2026 produced 4.85 billion port scan attempts - 19.2 million a day. The average router recorded roughly two port scan attempts every day, for the entire duration of the monitored period.

Scanning is not an attack in itself; it is a recon step that may precede one. And it is nearly the whole conversation: 90.1% of the attack stream this year was reconnaissance. The next-largest behavior - password bruteforcing - accounts for 8.7%.

PORTSCANNING

An automated probe asking an internet address which service “doors” answer — remote desktop on 3389, SSH on 22, camera and NAS interfaces beyond. A scan is reconnaissance, not a break-in: it builds the candidate list for whatever the operator runs next. Industrial scanners do this to every address, every day, forever.

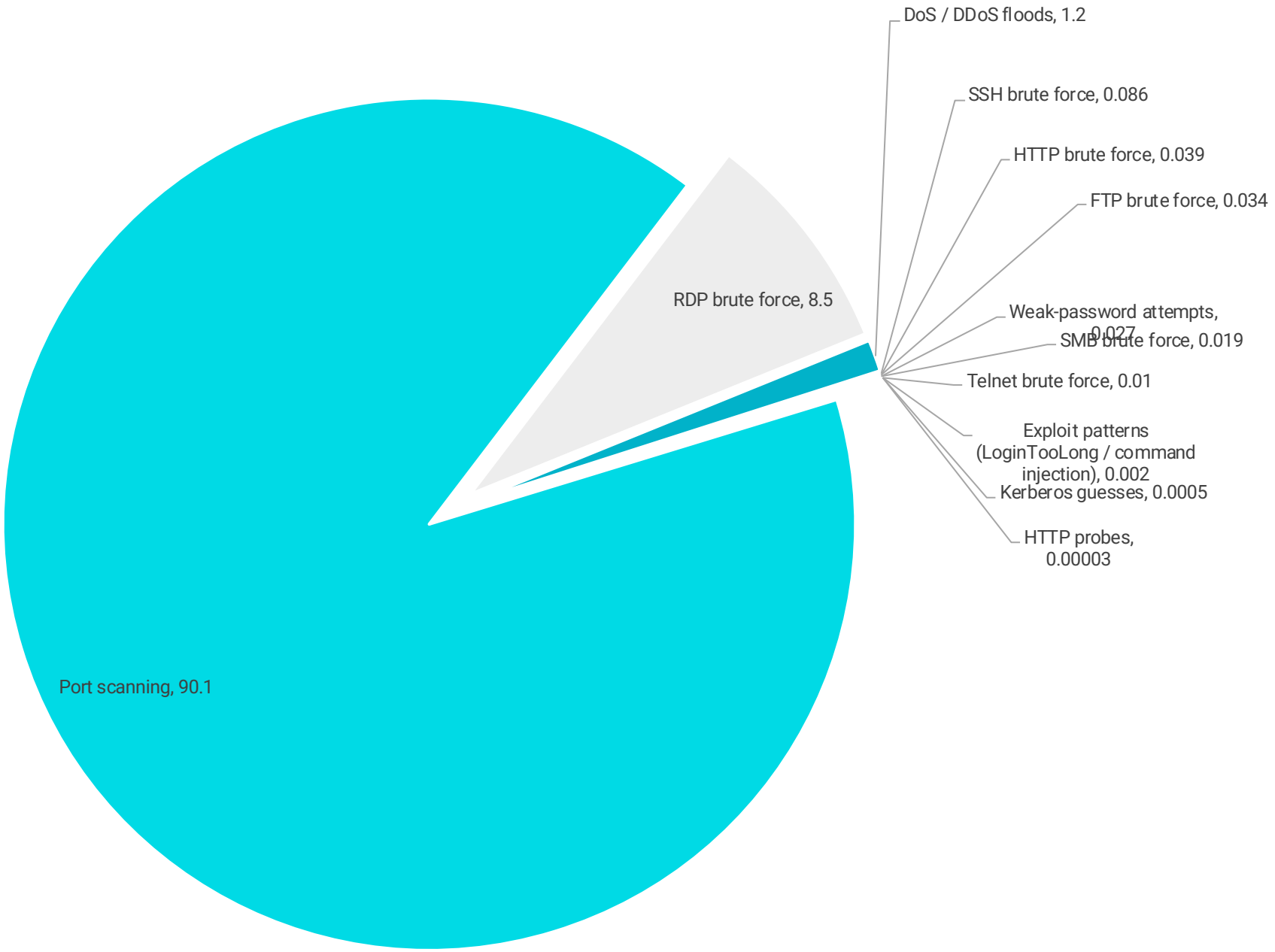
TOP ATTACKS

Port scanning dominate so completely that the rest of the attack stream has to be magnified to be seen at all.

4.85 billion scans, 90.1% of attack-category events - and 83.0% of absolutely everything our sensors logged this window.

Credential attacks come second. **466.6 million brute-force events, 8.7% of the stream.** 455.0 million aimed at RDP, the Windows remote-desktop service: 97.8% of all protocol-level password guessing. SSH, FTP, HTTP, SMB, Telnet and Kerberos divide the scraps in the single-digit millions.

The behavior practitioners call an exploit - matched LoginTooLong and command-injection patterns - appears **91,846 times. 0.002% of the stream.**



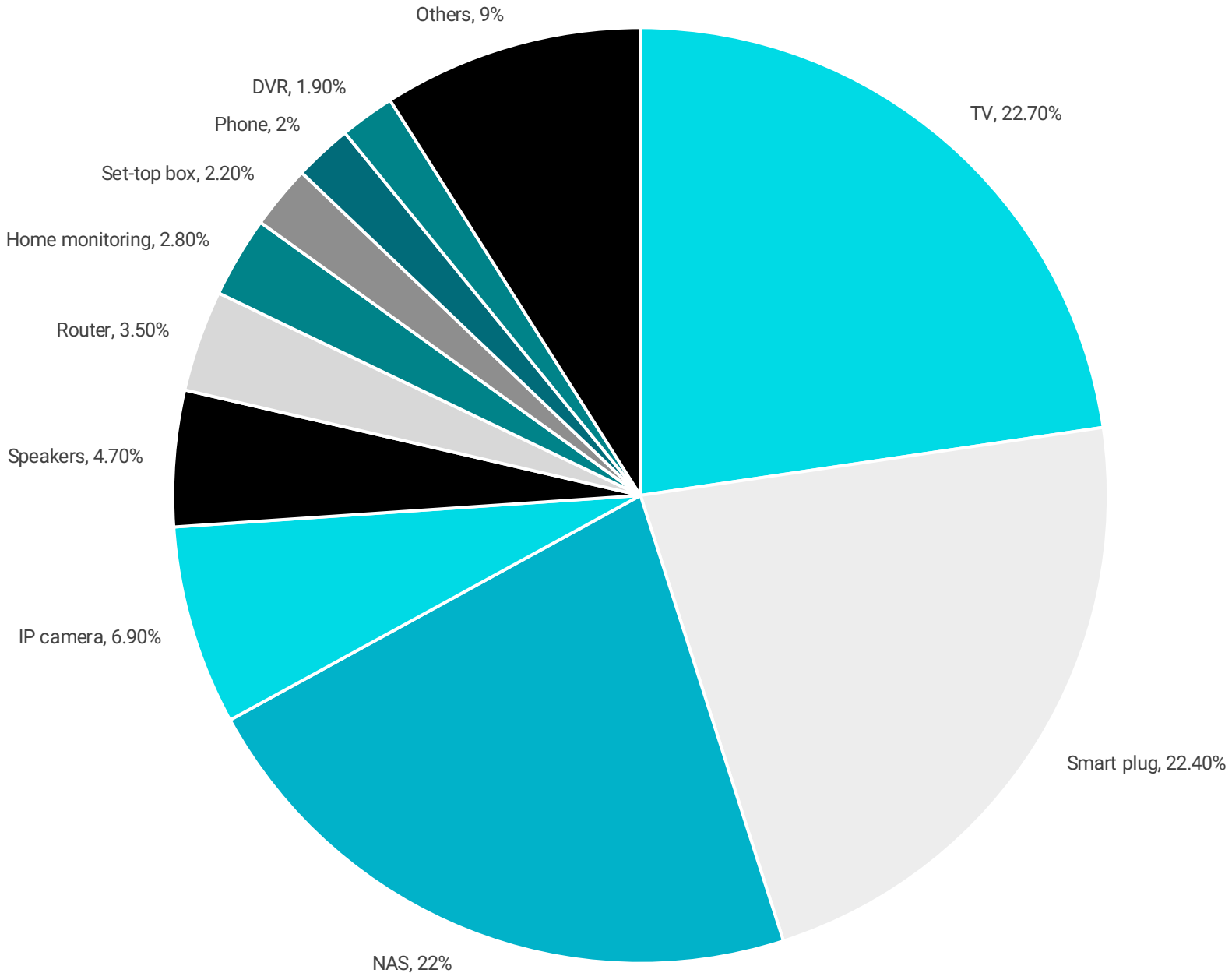
TOP VULNERABLE DEVICE FAMILIES

Smart plugs account for 266.7 million CVE observations in our window - the second largest device class in the dataset. Concentration inside the class is extreme, with a small number of devices dominating the model-level view.

Smart plugs are the emblematic lifecycle problem: cheap, invisible, configured once, and left in the wall long after their update window closes.

Four LG-branded labels in the top ten are one television family in naming variants; combined, LG labels account for 197.4 million observations - 16.6% of the CVE rollup (the privacy side of that screen: page 6).

Storage is the third pillar: MyCloud (153.8M), Synology (48.5M) and QNAP (23.3M) sum to 225.6 million — 18.7% of observations.



FROM BADBOX TO THE SECOND JOB

The BADBOX story covered in detail in the previous edition of this report was about cheap Android-based TV boxes and streaming sticks that reached consumers already infected, or that pulled in a backdoor through their first software update. Once resident, the malware turned the device into a residential proxy, an ad-fraud clickbot and a beachhead for subsequent operations.

The economics outgrew the takedowns. In its June 2025 public warning, the FBI put BADBOX 2.0 at more than a million compromised devices; Google moved against the advertising and distribution infrastructure around it. The playbook was criminal end-to-end: hidden code, no consent, monetized bandwidth and trust.

The smart-TV proxy SDK described by Spur reaches a recognizably similar outcome - the household's address moves somebody else's traffic - through what is presented as consent: an app, an EULA, a checkbox.

The mechanisms differ: BADBOX stole the connection; the SDK model buys it, cheaply, from users who may not understand what a residential proxy is. To the network, the two exits look identical.

SMART TV SETS

THE BIGGEST SINGLE SURFACE IN THE HOUSE

Televisions generate **270.3 million vulnerability observations** in our window, the largest count of any device class. One model label, the 2020 LG OLED C-series, is six years old and still appears 29.1 million times.

A TV spends most of its decade in the same place: online, idle, powerful enough to relay traffic, and - per this year's Gamers Nexus findings - already in the business of mapping its household. Old firmware keeps it exposed; a free app can rent its address.

The television is where this report's four roles converge in a single chassis: a **target** of record, a **sensor** with a microphone and an ACR engine, and - for whoever installs the right app - a **proxy** bolted to the wall.

Worth checking right now: check when the set left support, switch ACR and voice features to the minimum you actually use, and delete apps you no longer use.

SMART PLUGS

CONFIGURED ONCE, UPDATED NEVER

Smart plugs account for **266.7 million observations across our dataset**. The economics explain the security. A plug is the cheapest networked computer a household will ever buy; margins leave no budget for a patch pipeline, so end-of-sale usually means end- of-support.

The device then stays in the wall for years - streaming no video, running no apps, just holding an IP address and waiting. That profile - idle compute behind a trusted residential address - is exactly what botnets and proxy networks buy. A wall of these, unsupervised, is still infrastructure; it just isn't the owner's.

The quickest fix: this is the one device class where replacement costs less than remediation. If the vendor app is gone, the plug should be, too.

NAS DEVICES

THE FAMILY ARCHIVE WITH AN IP ADDRESS

Network-attached storage records **261.6 million observations**; three vendor lines - WD MyCloud (153.8M), Synology (48.5M) and QNAP (23.3M) - hold 18.7% of everything in the window between them.

A NAS is built to listen: full server stack, file and media services, remote-access features, admin panels - often on kernels years behind current. The product design is the exposure, and the public register keeps feeding it: NVD logged **48 QNAP CVEs** and 13 Synology CVEs in 2026 through late September.

Attackers read the same brochure their buyers did. A NAS holds the only copy of the photo library, runs 24×7, and sits inside the LAN with reach to everything - the purest “foothold” in the four-role framing of page 9, and a proven payload for ransomware operators.

Floor rule: keep the NAS off the open internet entirely - no UPnP ports, no exposed admin panel - and treat firmware updates as a subscription, not an option.

TOP CVES IN FIRMWARE

CVE	Description / Root Cause	Severity / Impact	Affected Component
CVE-2025-39905	A bug in the Linux kernel's network-link management code can cause two operations to wait for each other indefinitely.	CVSS 3.1 = **7 (High)**	Multiple versions affected
CVE-2025-38204	Out-of-bounds read vulnerability in the Journaled File System (JFS) implementation of the Linux kernel.	CVSS 3.1 = **7.1 (High)**	Multiple versions affected
CVE-2025-38704	Linux kernel vulnerability in the Read-Copy-Update No-Callback (RCU/NOCB) subsystem	CVSS 3.1 = **7.8 (High)**	Multiple versions affected

DEVICES BY VULNERABILITY TYPE

IoT insecurity stems from simplicity and scale. Overflow and DoS dominate across all device types, indicating poor memory safety and insufficient validation.

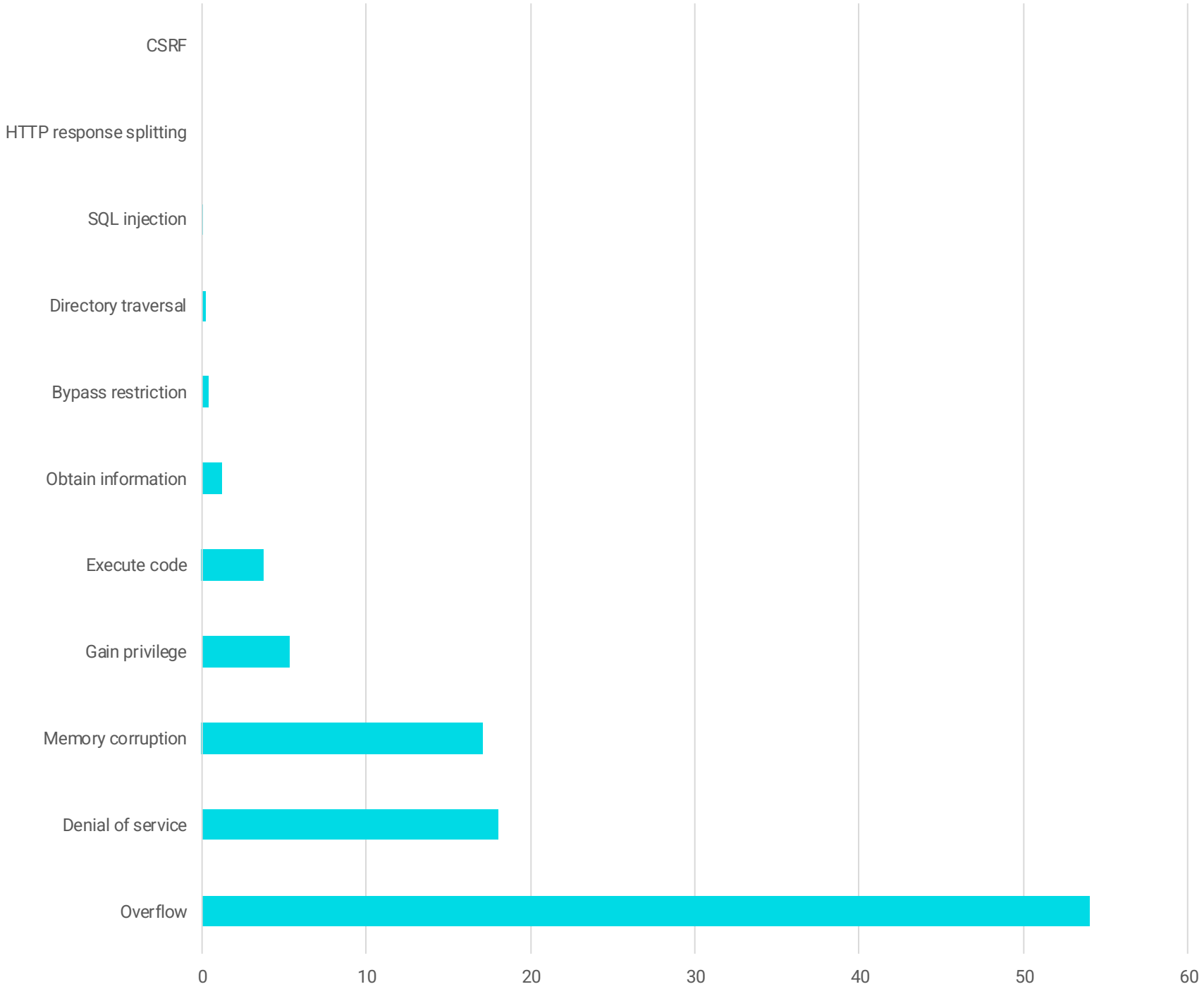
Devices meant to simplify life, like smart plugs, end up as the easiest entry points, while data-heavy appliances like NAS units become the most valuable targets.

TVs, NAS, and smart plugs together form the bulk of the modern IoT attack surface: complex, under-patched, and functionally essential, but often defenceless.

WHAT ATTACKERS TRY TO ACHIEVE

Overflow dominates by a huge margin (~54%) - bigger than every other category combined.

Adversarial capability is rare but qualitatively different: gain privilege (5.3%) + execute code (3.8%) + obtain information (1.2%) = ~10.3% of total. While small in numbers, these are the categories that map to attacker objectives



OBSERVATIONS AND TRENDS

The same three rooms of the house carry the load. Televisions, smart plugs and NAS appliances absorb 67.1% of all CVE observations. (page 15). What unites them is not chipsets or vendors but arithmetic: replacement cycles of five to ten years against support windows of two to four. Whatever else changes in IoT security, that gap decides where observations pile up.

Brute force has a monopoly platform: 97.8% of protocol-level password guessing targeted RDP (455.0 million of 466.6 million). Attackers spend their credential budgets on services that open a usable console; the entertainment hardware is collateral address space.

46.9% of CVE observations rate exactly 7.8 - the signature of a small number of common consumer firmware baselines scored once and inherited everywhere (page 25).

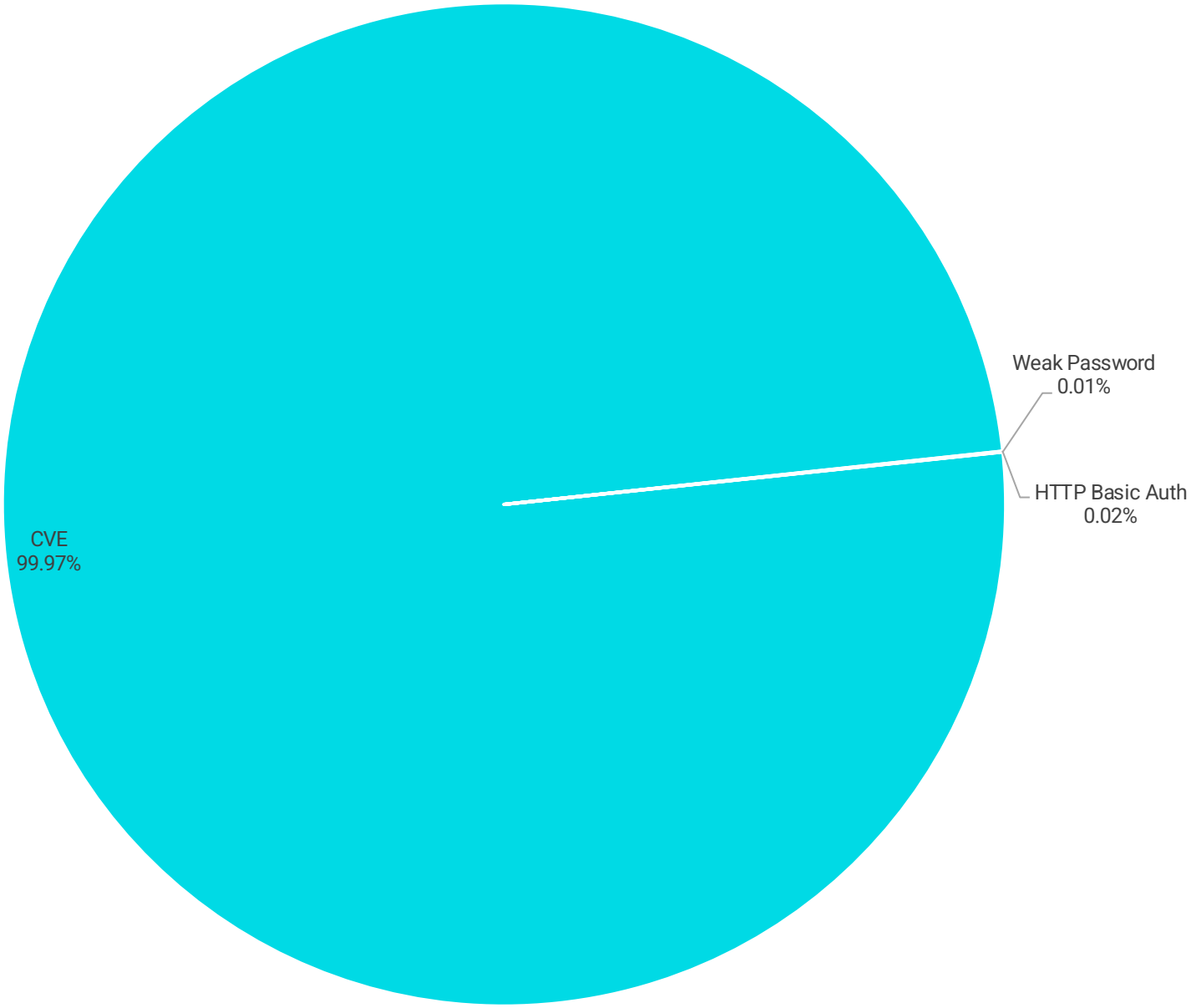
One vendor family can dominate a category. LG-branded TV labels - several naming variants of one platform - carry 197.4 million observations, 16.6% of the CVE rollup. The same TVs anchor this year's privacy reporting (page 6). The concentration is a brand artifact as much as a security artifact; we flag it rather than resolve it.

The ambient layer is structurally constant. Port scans were 93% of network-attack intercepts in the 2025 edition and 90.1% of the attack stream now, on a footprint roughly 71% larger. The pressure tracks the size of the window, not the news cycle.

VULNERABILITY TYPES AND RISK VALUES

Known (and fixed) CVEs represent the vast majority of IoT vulnerabilities. Only a fraction of attacks leverage weak passwords or plaintext authentication.

Looking closer at the CVE distribution, we see that most vulnerabilities are HIGH severity (CVSS 7.8) and depict a very common IoT baseline flaw.



A GUIDE TO IOT CVE OUTCOMES

CVSS SCORE*	% OF TOTAL	NOTES
7.0	15.5%	Entry floor of the matched set.
7.1	15%	Typically network-reachable with preconditions — adjacency, configuration or user interaction.
7.2	8.4%	(same group as 7.1/7.5)
7.5	3.6%	(typically network-reachable with preconditions)
7.8	46.9%	The spike — dominant consumer firmware baselines, inherited at scale.
8.8	2.4%	One notch from critical; often pre-auth, LAN/WAN-reachable classes.
9.1	0.5%	(same group as 9.3)
9.3	1%	Wormable classes under default configurations.
9.8	1.9%	Classic pre-auth remote-code-execution territory.
10	0.8%	Maximum severity — remote, low complexity, total impact.

*CVSS Scores are computed using CVSS 3.1, or Common Vulnerability Scoring System version 3.1, a standardized framework used to assess and communicate the severity of security vulnerabilities in software and systems. The rest of 4% in the CVSS mappings are values lower than 7.

LOOKING AHEAD AT 2027

1 Residential proxy operators will chase weaker oversight

In 2027, we expect residential proxy operators to expand distribution through inexpensive Android TV boxes, sideloaded apps and connected devices with less restrictive software ecosystems. As major TV platforms tighten enforcement, developers paid to bundle proxy software have an incentive to move to channels where scrutiny is lower. The attraction remains the household's internet connection: third parties can route traffic through a residential IP address, while the owner bears the bandwidth cost and potential consequences of abuse.

The indicator to watch is a shift in where proxy software appears, including alternative app stores, preinstalled software and devices sold under multiple unfamiliar brands.

2 Shared software flaws will produce security incidents that cross brand boundaries

In 2027, we expect more IoT vulnerability disclosures to implicate multiple brands because their products share firmware components, connectivity libraries or underlying hardware platforms. Attackers do not need to compromise a manufacturer's development pipeline to benefit from this concentration. A remotely exploitable flaw in a widely reused component can provide a common entry point into otherwise unrelated cameras, recorders and smart-home products.

The resulting exposure will depend on how quickly each manufacturer delivers a working fix. Watch for coordinated disclosures covering multiple vendors, followed by uneven patch availability that leaves some products vulnerable after others have been repaired.

3 Smart-home privacy investigations will follow data across devices and accounts

In 2027, we expect greater scrutiny of how television viewing data, connected-device activity and linked consumer accounts combine into household profiles. Individual permissions reveal only part of this picture. Understanding the privacy impact requires tracing which companies receive the data, how they connect it with other information, and whether consumers can disable those uses without losing core device functions.

The indicator to watch is research and enforcement focused on data sharing between device manufacturers, advertising platforms and commercial partners. Privacy assessments will increasingly examine the full data relationship, rather than stopping at whether a microphone is active or a television collects viewing history.

HOW TO STAY SAFE

In our experience, many smart home compromises are linked to outdated, misconfigured, or abandoned devices. Security demands visibility and continuous device monitoring.

- Update the router twice a year, on a schedule. The router is the perimeter this whole report is measured from — 10.4 million of them generated every number here. Firmware that never updates is the single largest avoidable risk.
- Retire devices past their support window - especially the cheap ones. The plug and TV classes dominate our vulnerability charts (67% of observations with NAS, page 12) precisely because they outlive their patch windows in silence. A $20 plug past end-of-life is a $20 lesson, not an heirloom.
- Keep device services off the open internet. No exposed admin panels; UPnP off at the router; the NAS stays LAN-only - the class holding 18.7% of all observations should not be answering strangers
- Use unique passwords; kill factory defaults. 466.6 million credential events this window — 97.8% of protocol guesses aimed at remote-desktop doors — reward default-password hygiene more than any other habit.

A ROUTER THAT WATCHES THE WHOLE HOUSE

The four roles described on page 10 - target, proxy, sensor, foothold - all assume a stable boundary between the home network and the rest of the internet. That boundary is the home router, and the threats described across this report all run through it.

NETGEAR Armor puts a security layer inside that boundary. Powered by Bitdefender, the platform combines network-level threat detection with vulnerability and device-fingerprinting technologies across the household - including the device classes this report names most often: televisions, smart plugs, NAS devices and IP cameras.

A modern home-security layer needs to see all four roles, identify the device in each case, and provide the household owner with the evidence to act.

Disclosure: Bitdefender provides the security technology that powers NETGEAR Armor and has a commercial interest in its distribution. This report was prepared using Bitdefender and NETGEAR telemetry.

I. General Disclaimer Regarding the Nature and Purpose of the Report

This report serves an exclusively informational and educational purpose. It does not constitute and does not replace legal, financial, investment, or any other form of professional advice. The information contained in this document reflects how Bitdefender has analyzed and interpreted its own technical data (telemetry) and should not be treated as absolute truths or as a complete picture of digital threats worldwide.

The report is published in good faith, to raise awareness of online threats and to contribute to a safer digital environment. Bitdefender does not warrant that the information is accurate, complete, or up to date, and assumes no responsibility for decisions that readers may make based on this report.

II. Disclaimer Regarding Methodology and Data Limitations

The data in this report originates from Bitdefender's proprietary systems (telemetry), collected between January 2026 - September 2026, through the company's products and services. They reflect only what Bitdefender was able to observe through its own infrastructure and do not represent a complete picture or an official statistic of IoT threats at the global, regional, or national level.

Estimates and projections are based on internal analytical models, which may have limitations - for example, incomplete samples, selection bias, or variations over time. The figures and percentages in the report should be read as indicative markers, not as exact measurements.

When we classify messages, links, calls, or advertisements as "risky," "malicious," or "fraudulent," we do so based on automated technical criteria. This does not mean that they automatically constitute criminal offenses or regulatory violations from a legal standpoint - only judicial and regulatory authorities can make such a determination.

III. Disclaimer Regarding Personal Data Protection

Bitdefender processes the analyzed data in compliance with the European data protection regulation

(GDPR - Regulation (EU) 2016/679), applicable national legislation, and internal privacy policies. All data presented in the report is aggregated and anonymized - in other words, no individual can be identified based on the published information.

IV. Disclaimer Regarding Third Parties Mentioned in the Report

When we mention platforms, companies, brands, public figures, or authorities in this report, we do so solely to describe and document the phenomenon from a cybersecurity perspective. We do not accuse or suggest that these entities have violated the law or bear any fault.

The fact that we mention them in the report does not mean that we consider them involved, complicit, or negligent in connection with the situations described.

All trademarks, trade names, and logos mentioned belong to their respective owners and are used solely for identification and reference purposes

V. Disclaimer Regarding Statements Related to Public Authorities and Third-Party Reporting

Information about the actions of public authorities referenced in this report — including Slovakia's National Security Authority (NBÚ), the United States Cybersecurity and Infrastructure Security Agency (CISA), the United States Federal Bureau of Investigation (FBI), and Iran's Supreme Council of Cyberspace- as well as the third-party reporting cited (including the Financial Times, Spur and Gamers Nexus) — originates from public sources: official reports, press releases, advisories, and journalistic articles. Bitdefender has not independently verified the accuracy or completeness of this information and does not express opinions on the legality, proportionality, or effectiveness of the respective authorities' actions.

VI. Disclaimer Regarding Limitation of Liability

To the maximum extent permitted by law, Bitdefender, its affiliated companies, directors, employees, and collaborators shall not be liable for any damages - direct or indirect, foreseeable or unforeseeable - that may result from the use, interpretation, or inability to use the information contained in this report. This limitation applies regardless of the legal basis invoked (contract, tort, strict liability, or any other ground, but does not apply to damage caused intentionally or through gross negligence, or where liability cannot be determined under mandatory law.

VII. Disclaimer Regarding Governing Law and Jurisdiction

This report and any disputes related to its content are governed by Romanian law. Any litigation shall be resolved exclusively by the courts of Bucharest, Romania, subject to any applicable mandatory rules of private international law. Nothing in this section deprives consumers of the protection of mandatory provisions of the law of their habitual residence or of their right to bring proceedings before the courts of that place.

VIII. Disclaimer Regarding Updates and Validity of Information

The information in this report is valid as of the date of publication and reflects what was known at that time. Bitdefender is under no obligation to update, revise, or correct the report after publication. Cybersecurity threats evolve rapidly, and the data presented herein may become outdated or inaccurate over time.

Bitdefender®
WWW.BITDEFENDER.COM/IOT