Bitdefender

WHITEPAPER

Router Protection

Protecting Modern Routers on Auto-Pilot

Trusted. Always.

Contents

Introduction

Most home routers are vulnerable, according to the American Consumer Institute - Center for Citizen Research. Their research analysis[1] shows that of 186 sampled routers, 155 (**83%**) were vulnerable to potential cyberattacks. The sampled routers were from 13 popular manufacturers, including Linksys, Belkin, D-Link, and others.

Affected routers often become nodes in botnet armies that launch Distributed Denial of Service (DDoS) attacks. This translates into increased costs for operators, due to increased customer support load and abnormally high bandwidth consumption during attacks.

Additionally, personal data and financial credentials get stolen as a result of attacks that start on the router. In this troubled environment, Internet Service Providers are increasingly looking to offer home security solutions to fill the gap and keep subscribers safe.

> **For providers of connectivity, Bitdefender offers the security & privacy layer that delivers safe, optimal and seamless experiences for subscribers, so they can enjoy digital experiences without issues.**

Bitdefender Router Protection protects the router from attacks coming from any direction (Internet/LAN). By integrating the agent into home routers, it pulls continuous security patches, relieving you as an operator from the pressure of delivering firmware updates when new vulnerabilities are found.

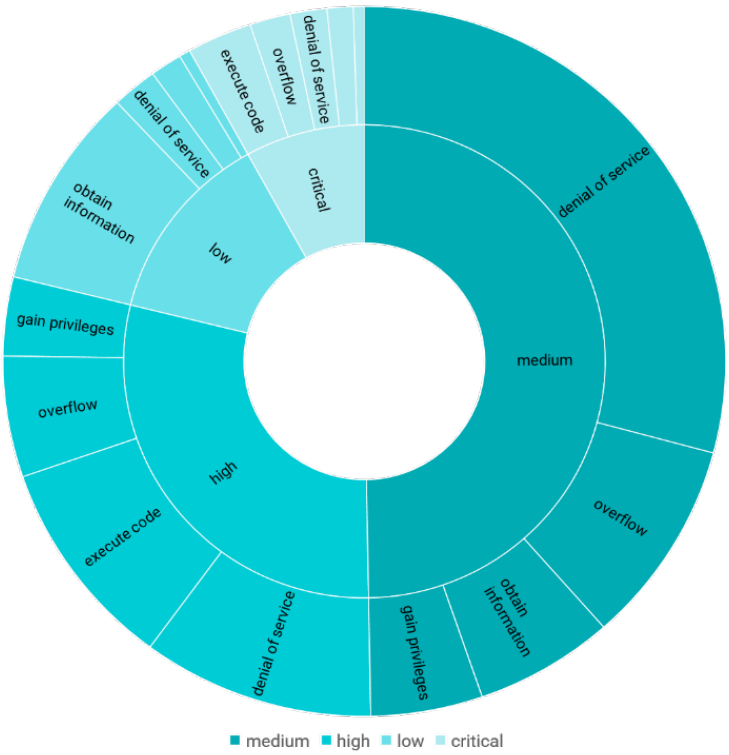


Figure 1 - Vulnerabilities & risks

A Multi-Layered Approach to Protect Consumers

In order for a modern home to be properly protected, it needs multiple layers of protection:

Service Provider Protection

Internet Service Providers use complex enterprise security solutions to protect their network and routers. Before any Internet traffic is sent to a home router or gateway, it already goes through the security protocols in place inside the ISP's infrastructure.

Sometimes these security protocols are difficult to put in place and might also affect general quality of service (e.g. slow Internet, restricted ports or unavailable services). Because of this delicate balance between security and customer experience, some providers are perceived to offer a better Internet service, often prompting consumers to switch between providers.

1 https://www.theamericanconsumer.org/wp-content/uploads/2018/09/FINAL-Wi-Fi-Router-Vulnerabilities.pdf

Router Protection

The Internet connection feeds into the home router, the central gateway for all household devices. Some premium routers come with advanced features, but most have just a basic level of security. Making sure your customer-premises equipment (CPE) is protected prevents your customers' Internet experience from degrading when cyberattacks happen.

Because all incoming and outgoing network traffic inside the smart home goes through the router, it makes it the ideal candidate to fortify subscribers' households. **Bitdefender Router Protection is targeted towards protecting home routers from complex cyber attacks.**

IoT & Endpoint Protection

Incoming connections eventually reach household devices such as laptops, phones, tablets, smart gadgets or appliances. No single security solution that can provide 100% protection, so there is a chance malware reaches consumer endpoints. This is why it's highly recommended that consumers also install protection software on their supported devices.

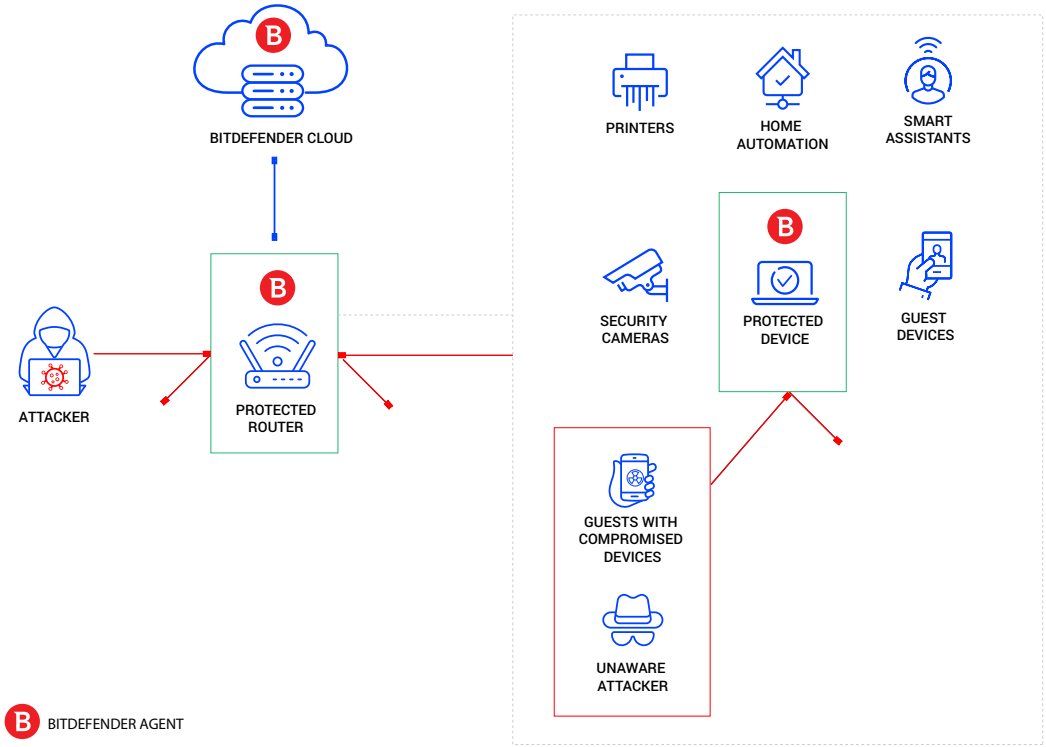
Bitdefender offers service providers a separate solution to protect consumer devices in the home, called the Bitdefender Subscriber Protection Platform. It protects both smart IoT devices running proprietary OS's, as well as Windows, macOS, Android and iOS devices.

> **Bitdefender is the only cybersecurity provider that has solutions to protect both the router and the devices connected to it from malicious attacks.**

Router Protection Overview

Bitdefender Router Protection uses a lightweight agent* that runs on the router to protect it against attacks coming from both within the home network, and from the open Internet.

At its core, it uses the Bitdefender Global Protection Network to prevent exploits, stop brute force attacks, and prevent rogue devices from participating in DDoS attacks.



*The agent works on any router or IoT device that has at least 20MB available disk space, 100MB of RAM and at least 800MHz CPU. It currently supports CPUs architectures such as ARMv7, ARMv8, and MIPS.

Benefits

Live Virtual Patching

To prevent exploitation attempts of existing vulnerabilities, **Bitdefender Router Protection implements a virtual patching method for home routers**. The remediation of the source code is still advisable, but it's not always possible to deploy updates or hotfixes fast enough. It's good practice to run both strategies in tandem, as they are not mutually exclusive.

Virtual patching works by checking commands on the router against CVEs in the Bitdefender Global Protection Network. Many attacks rely on command injection, local file inclusion or directory traversal exploits to cause overflows and gain persistent privileges. Bitdefender Router Protection keeps malicious code from executing on the router, so that even if the firmware is not up-to-date, consumer equipment will still be safe.

Protect Your Consumer-Premises Equipment (CPE)

According to Bitdefender telemetry[2], routers rank as the #3 most vulnerable device in the home. We already showed in the introduction of this paper that 83% of routers installed in consumers' homes have vulnerabilities. What's even more worrying is that, according to our data, 75% of these threats have medium or high impact.

Bitdefender Router Protection mitigates the risks of denial of service, remote code execution, or brute-force attacks. Because the router agent synchronizes with our Global Protective Network, your equipment is protected against zero-day threats with no intervention or updates on your behalf.

Better Connectivity

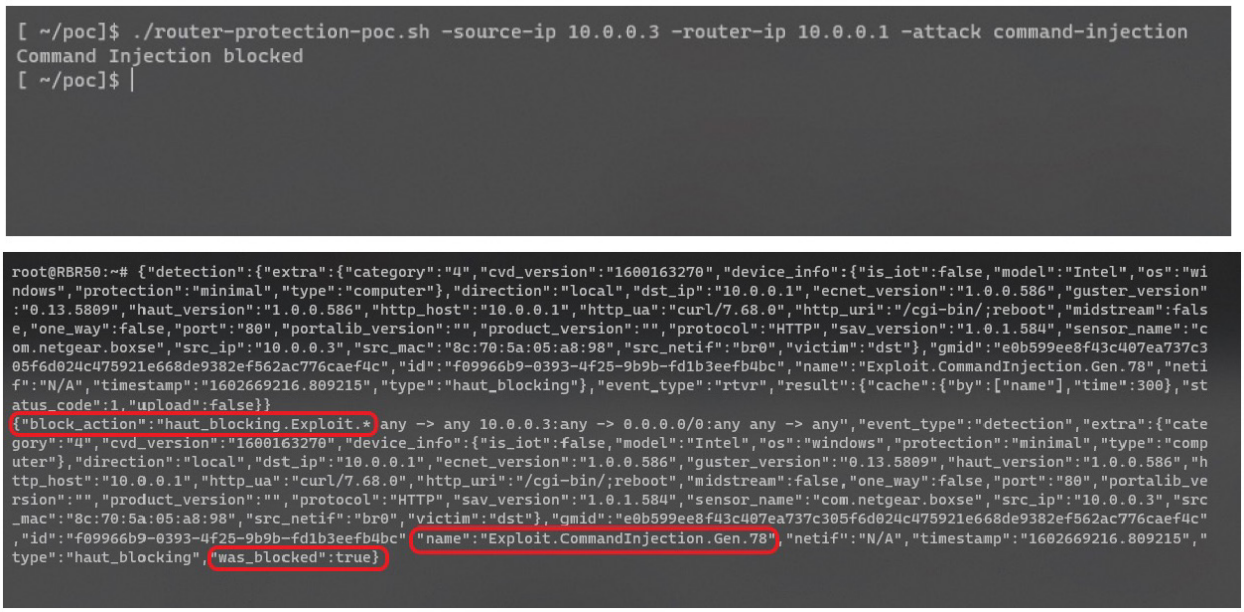
Disruptive attacks can lead to temporary loss of connectivity for consumers. In the context of widespread remote work policies, this is more than just an inconvenience – it's a worst-case scenario. Network congestion or devices going rogue are enough to prompt support calls and a degradation of consumer loyalty towards you as a service provider.

Bitdefender Router Protection helps ensure better connectivity by securing the router itself, and in some cases prevents complete loss of connectivity for the consumer.

Features

Exploit Prevention

Bitdefender Router Protection offers an intelligent **Intrusion Detection and Prevention System (IDS/IPS)** that protects its host against even the newest vulnerabilities. It covers multiple types of vulnerabilities, including command injection, local file inclusion and directory traversal.



Example of a blocked command injection exploit

2 https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf

Thanks to this IDS/IPS-like technology, users are no longer required to update their firmware in order to be protected. The Bitdefender agent gets live updates from our Global Protection Network, giving Service Providers and router manufacturers the time they need to release an official patch.

Brute Force Protection

The most common type of attack on IoT devices is the Brute Force attack, and routers are no exception. But **routers protected by Bitdefender Router Protection will not be impacted by brute force attacks**, and will not be easily targeted to become part of botnet armies. Our technology covers a wide range of protocols, such as FTP, SSH, Telnet, SMB, or HTTP.

DDoS Protection

The number of smart (IoT) devices connected to Internet is growing fast, but many device manufacturers are focused on developing new functionalities while neglecting security altogether. In this context, we are talking about a very large number of devices that are no longer receiving firmware updates, are vulnerable to exploits and are already "soldiers" in botnet armies that perform attacks over Internet.

Many botnets are behind DDoS attacks. When multiple devices generate large amounts of traffic towards a specific target, they not only affect the target, but also the infrastructure they run on, by clogging it with useless traffic.

The router in particular is essential for connectivity throughout the home. With Bitdefender Router Protection on, this key component becomes a protected device (similar to a traditional endpoint running an AV solution), safe against attacks coming from any direction. It even works if a family guest with a compromised device connects to the home network, and it's especially useful for small businesses such as coffee shops or restaurants, which have public Wi-Fi networks to which any customer can connect to.

The types of DDoS attacks that are blocked include TCP.Flood, Syn.Flood, and Ping.Flood.

ISP Challenges

1. If part of a larger attack, the amount of generated traffic is not always detected by ISP safeguards.

2. **Network bandwidth consumed by junk traffic**.

3. Blocking Internet access for an entire household.

Customer Experience

1. Degraded Internet experience during DDoS attacks, as some services might stop working.

2. Affected router might become unresponsive or experience malfunction.

3. Needs assistance to troubleshoot issues; **no Internet access until the attack is over**.

Delivering Home-Centric Security

Why Bitdefender is the right partner for you

Choose Bitdefender to gain access to high-tech security features and valuable go-to-market strategies.

We'll help you talk security & privacy to your customers to build long-term, high-value relationships. Our products consistently rank #1 in consumer tests and have a history of proven excellence.

And because Bitdefender protects both you as service provider and your customers alike, you can provide a safer online experience, while also opening new revenue streams.

Conclusion

Whether it's stealing money or data, attackers will go wherever they can — and the new frontline is the smart connected home. Bitdefender Router Protection is a necessary protection layer for service providers that want to build long-term loyalty with a secure home environment for their customers.

Benefits of using Bitdefender technologies for connectivity providers

- Protect Your Network
- Your core network will benefit from protection against DDoS attacks on routers, while saving costs due to decreased bandwidth.
- Decrease Costs
- Decrease the number of customer support calls and reduce costs with technician visits as a result of infected routers.
- Shorten Response Time for New Vulnerabilities
- Gives you time to implement and deploy security patches at your own pace: our Router Protection auto-updates with patches for new threats in a matter of days.

Beyond Router Protection...

- Increase ARPU With a IoT Protection
- Bitdefender Subscriber Protection Platform, our ecosystem of value-added services (VAS), can increase your average revenue per user (ARPU) by up to $99/year.
- Increase Customer Loyalty
- With a whole range of security issues taken care of, your customers benefit from a safer online experience that will increase loyalty and reduce churn.

To learn more about the Bitdefender IoT ecosystem, visit our website today.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Bitdefender-IOT-Whitepaper-RouterProtection-creat7309-en_EN
CD-10/19/23 • MD-October 24, 2023 11:26 pm