2024 DUBLIN

2 - 4 October, 2024 / Dublin, Ireland

OPEN BY DEFAULT: THE HIDDEN COST OF CONVENIENCE IN NETWORK SECURITY

Aurelio Picón López

CUJO AI, Hungary

aurelio.picon@cujo.com

www.virusbulletin.com

ABSTRACT

This paper stems from an eye-opening realization after spending a year analysing anonymized network security event logs from over two billion devices across North America and Europe. My work involved tracking malware, monitoring trends in tactics, techniques and procedures (TTPs), assessing IoT software updates, identifying targeted devices, and observing botnet behaviours. Throughout this process it became clear that the default setting of auto port forwarding in household routers is a significant factor in the spread and operation of botnets.

In this paper and the accompanying talk, I will present statistical data gathered during my daily threat research that supports this claim. We will explore how UPnP (Universal Plug and Play) and its default auto port forwarding setting contribute to household network vulnerabilities.

Additionally, I will share empirical data on the status of UPnP settings in real users' routers, collected through user surveys on social media and analysis of default configurations from ISP-deployed routers. This data highlights how common and impactful these default settings are in real-world scenarios.

Finally, this paper will conclude with a call to action for security-conscious IT professionals. By raising awareness and advocating for changes in default network settings, we can significantly improve household security and reduce the prevalence of botnet activity.

INTRODUCTION

The rise of internet-connected devices has brought incredible convenience to our daily lives. From smart TVs and home security cameras to routers and network-attached storage, these devices make our homes more connected and our lives easier. One technology that plays a big role in this seamless connectivity is Universal Plug and Play (UPnP). UPnP is a set of networking protocols that allow devices on a local network to automatically discover and interact with each other without manual setup. This makes it simple for users to connect devices like printers, gaming consoles and smart home systems.

However, the convenience provided by UPnP comes with hidden security risks. UPnP often comes enabled by default on many routers and IoT devices. While this default setting simplifies device connections, it also creates opportunities for potential security breaches. Attackers can exploit these open connections, leading to compromised devices and networks.

This paper explores the unintended consequences of UPnP's default settings and highlights how they negatively contribute to the internet security landscape. We'll look at the data and real-world examples to understand the extent of these risks and consider why rethinking these default settings is crucial for improving network security in households.

OVERVIEW OF THREAT ACTORS

Threat actors exploiting network vulnerabilities can be categorized into three main groups: state-sponsored groups, financially motivated cybercriminals, and hacktivists. There follows a detailed overview of each group with a couple of samples for illustrative purposes.

State-sponsored groups

State-sponsored threat actors are typically funded and directed by nation-states. Their primary goals are espionage, cyber warfare, and political disruption. These groups possess advanced capabilities, significant resources, and long-term objectives.

- **APT28 (Fancy Bear)**: a Russian military intelligence unit known for its sophisticated cyber espionage campaigns. APT28 targets government entities, political organizations and military sectors, using spear-phishing, zero-day exploits and malware to gain access to sensitive information.
- **APT29 (Cozy Bear)**: another Russian intelligence group, APT29 focuses on long-term espionage missions. They employ advanced persistent threats (APTs) to infiltrate networks and remain undetected for extended periods. Their targets include government agencies, research institutions and healthcare organizations.

Financially motivated cybercriminals

This group of threat actors aims to generate profit through cybercrime. They exploit vulnerabilities for financial gain, often through methods such as ransomware, data theft and fraud.

- **FIN7 (Carbanak)**: a sophisticated cybercriminal group that targets financial institutions and retail sectors. FIN7 uses spear-phishing campaigns and custom malware to steal credit card information and conduct fraudulent transactions, causing significant financial losses.
- **TrickBot Group**: initially a banking trojan, TrickBot evolved into a versatile malware platform used for data theft, ransomware distribution, and as an entry point for other malware. The group frequently targets financial institutions and large enterprises.

Hacktivists

Hacktivist groups engage in cyber activities to promote political, social or ideological agendas. Their attacks are often disruptive but can also cause substantial damage to their targets.

- **KillNet**: a hacktivist group known for conducting distributed denial-of-service (DDoS) attacks and defacing websites. KillNet targets entities that oppose its ideological views, including governments, corporations and organizations. They use compromised devices and botnets to amplify their attacks.
- **Anonymous**: a decentralized group of hacktivists that conduct cyber operations in support of various causes, such as anti-censorship, anti-corruption, and human rights. Anonymous uses DDoS attacks, website defacements and data leaks to draw attention to its causes and pressure its targets.

CASE STUDY: KILLNET

Background

KillNet was a hacktivist group that gained notoriety for its disruptive cyber attacks. Unlike financially motivated cybercriminals or state-sponsored groups, KillNet focused on ideological and political objectives. The group's primary method of attack was through DDoS attacks, which aimed to overwhelm and disable targeted websites and online services.

Tactics and methods

- **DDoS attacks**: KillNet uses DDoS attacks to flood targeted servers with traffic, causing them to crash or become inaccessible. These attacks are often carried out using botnets – a network of compromised devices controlled remotely by the attackers.
- **Website defacement**: in addition to DDoS attacks, KillNet sometimes defaces websites, replacing their content with messages that promote the group's ideological views.
- **Exploitation of vulnerabilities**: KillNet identifies and exploits vulnerabilities in publicly exposed endpoints, often through brute force attacks or dictionary attacks to gain access to these systems.

Notable incidents

- **Bulgaria**: KillNet targeted several Bulgarian government websites with DDoS attacks, causing significant disruptions to online services. These attacks were part of a broader campaign against countries supporting certain political positions.
- **Bermuda**: The group launched a series of DDoS attacks on Bermuda's financial institutions, leading to temporary outages and operational disruptions. This attack highlighted KillNet's ability to impact critical infrastructure.
- **DDoS attack against Royal Family website**: in October 2023, KillNet launched a DDoS attack on the official website of the British Royal Family, causing it to go offline for several hours. This attack was part of KillNet's broader campaign to disrupt high-profile targets and gain attention.

Correlation with botnet activity

KillNet's attacks often coincide with spikes in botnet activity. Analysis of network traffic reveals that significant increases in botnet command-and-control communications usually occur just before KillNet's high-profile DDoS attacks. For example, before the group's attack on the British Royal Family's website, there was a notable surge in botnet traffic.

The graphic shown in Figure 1, mapping IoT botnet activity, correlates directly with known public activity of the threat actor.

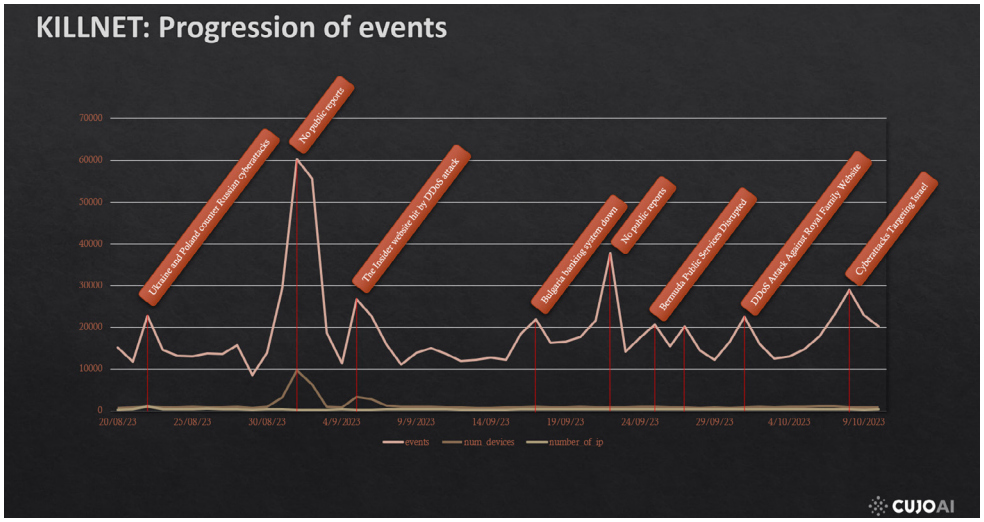

Figure 1: IOT botnet activity.

This pattern underscores the reliance of threat actors on botnets to execute their operations. Disrupting these botnets and preventing their spread is crucial in diminishing the capacity of groups like KillNet to launch large-scale cyber attacks.

REMOTE ACCESS TARGETED HOUSEHOLDS STATISTICS

To illustrate the impact of UPnP on household network security, we analysed anonymized network security events from over three billion devices. Our focus was on remote access events, which often serve as a gateway for unauthorized access and subsequent malicious activities. We present three key insights derived from this data.

Graph 1: Remote access events by environment

Figure 2 shows the percentage of households that experienced at least one incoming remote access event over a one-week period across six different environments. Notably, two environments – where UPnP is enabled by default – show over 50% of households experiencing remote access events. In contrast, the other four environments, where UPnP is disabled by default, each have 10% or fewer households with such events. This stark difference highlights the security risks associated with having UPnP enabled by default.

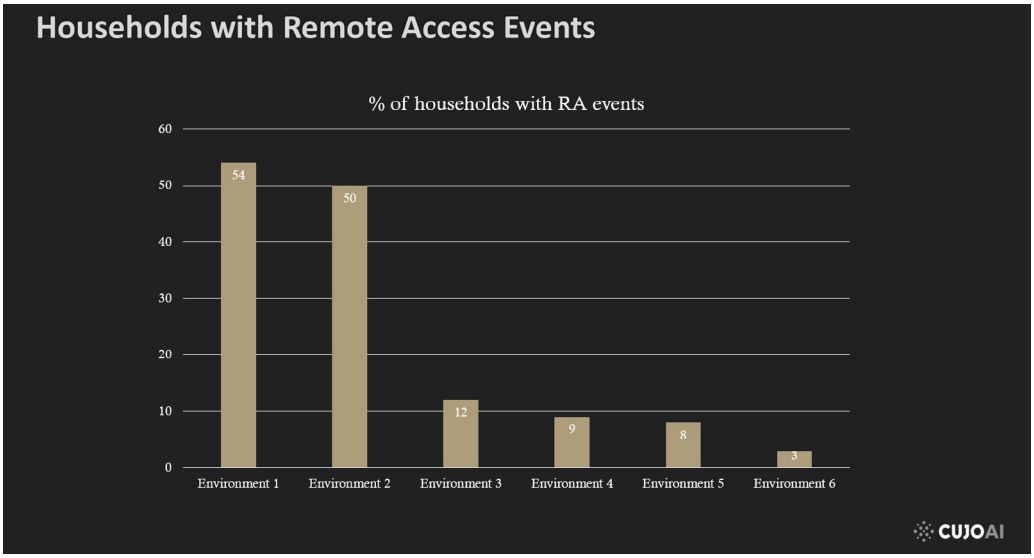

Figure 2: Percentage of households that experienced at least one incoming remote access event over a one-week period.

Graph 2: Distribution of remote access events (UPnP enabled by default)

In environments where UPnP is enabled by default, a significant portion of households – over 50% on average – have experienced at least one remote access event. Figure 3 underscores the widespread exposure to potential threats in these settings, where devices can automatically open ports without user intervention or awareness, increasing the risk of unauthorized access.

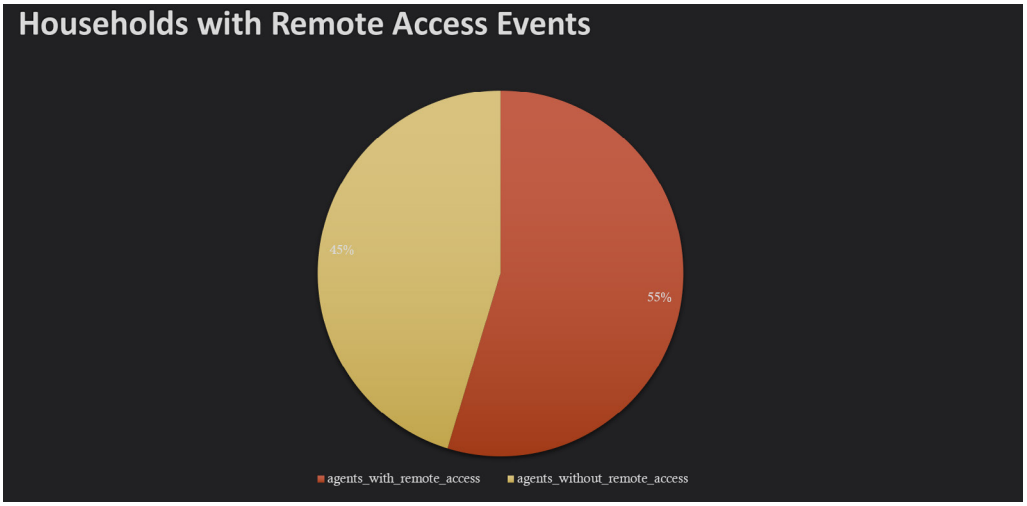

Figure 3: Households with remote access events where UPnP is enabled by default.

Graph 3: Distribution of remote access events (UPnP disabled by default)

Conversely, in environments where UPnP is disabled by default, most households – over 90% – did not experience any remote access events. This distribution demonstrates the protective effect of having UPnP disabled by default, reducing the avenues through which remote access can be exploited.

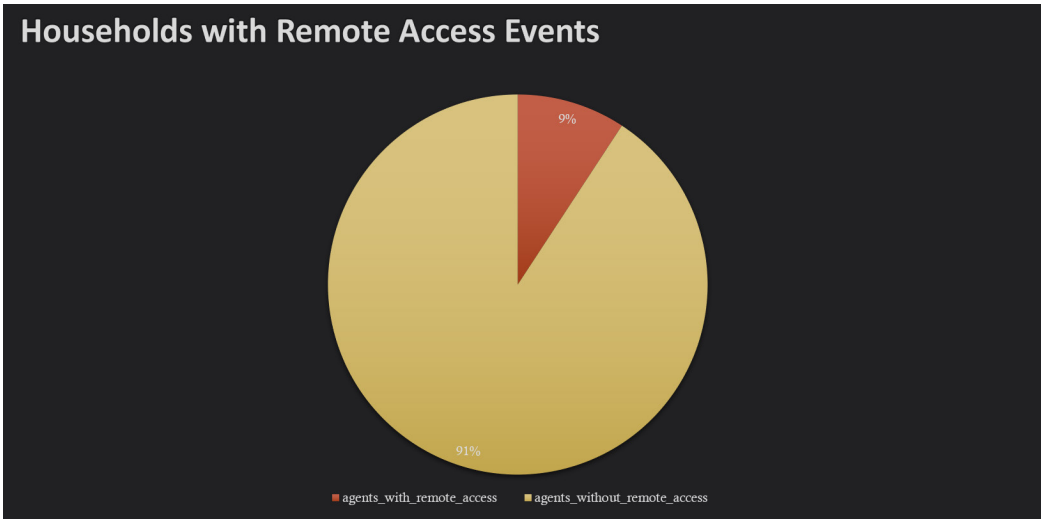

Figure 4: Households with remote access events where UPnP is disabled by default.

COMPROMISED DEVICES: THREAT ACTOR SWISS ARMY KNIFE

Compromised devices have become a critical part of the infrastructure used by threat actors, acting as a distributed and powerful platform for launching a wide range of cyber attacks. Much like the way in which legitimate cloud services provide scalable resources for businesses, these compromised devices offer cybercriminals a flexible and robust 'cloud infrastructure' to conduct their operations. Whether through individual devices hijacked within household networks or vast botnets composed of millions of such devices, the role of compromised hardware in supporting and amplifying malicious activities cannot be overstated. This section provides a light exploration of how compromised devices function as the backbone of cybercriminal enterprises and the diverse ways in which they are exploited.

Botnets

Botnets, composed of numerous compromised devices, are the go-to tool for cybercriminals due to their versatility and power. These networks enable attackers to conduct extensive and coordinated operations across many devices simultaneously.

- **Launching DDoS attacks**: botnets can flood targeted servers or networks with overwhelming amounts of traffic, causing disruptions and rendering services unavailable.
- **Creating proxy networks**: compromised devices act as intermediaries, masking the origin of malicious traffic and providing anonymity for cyber attacks or illicit activities.
- **Cryptocurrency mining**: attackers install mining malware on compromised devices, utilizing their processing power to mine cryptocurrencies covertly.
- **Email spam campaigns**: botnets are employed to send vast quantities of spam or phishing emails, concealing the true source of these messages, and facilitating large-scale scam operations.
- **Ransomware and malware distribution**: botnets serve as distribution hubs for ransomware and other malware, leveraging compromised devices to propagate infections widely.
- **Surveillance and espionage**: devices with cameras and microphones are exploited for unauthorized surveillance, capturing sensitive audiovisual information.
- **Data theft**: attackers extract personal or sensitive data stored on or transmitted through compromised devices, including passwords, financial details, and proprietary information.
- **Network infiltration**: compromised IoT devices can act as entry points into a network, allowing attackers to move laterally and target high-value assets.
- **Credential stuffing**: botnets automate login attempts using stolen credentials, aiming to breach accounts and systems across various websites.

- **Ad fraud**: attackers use compromised devices to perform click fraud or inject ads, generating illicit ad revenue.
- **Identity spoofing**: cybercriminals exploit legitimate devices to gain unauthorized access by spoofing identities.
- **Manipulating physical systems**: in industrial environments, compromised IoT devices can be manipulated to disrupt operations or cause physical damage.

UPnP MAIN BENEFITS AND VULNERABILITIES

Universal Plug and Play simplifies network connectivity by allowing devices to automatically discover and interact with each other. While UPnP as a protocol encompasses a range of functionalities, this section focuses specifically on its auto port forwarding feature, which automatically manages network port configurations. This capability is both a major convenience and a significant security concern.

Benefits of auto port forwarding with UPnP

- **Automatic configuration**: UPnP's auto port forwarding allows devices to configure network ports without manual intervention. This means that when you connect a new device, such as a gaming console or a media server, it can automatically request the necessary ports to be opened on the router. This ease of setup is particularly beneficial for non-technical users, as it reduces the complexity involved in configuring network services.
- **Dynamic response to devices**: with UPnP, devices on the network can dynamically request and manage their own port forwarding rules. As devices power on and off, or as applications start and stop, UPnP can adjust the network configuration in real time. This flexibility supports seamless operation of applications that require specific ports to be accessible, such as video conferencing tools or remote desktop applications.
- **Temporary open ports**: unlike manually configured port forwarding, which often leaves ports open indefinitely, UPnP can open ports only for the duration that they are needed. Once a device or service no longer requires the port, UPnP can automatically close it, potentially reducing the window of exposure to external threats.

Vulnerabilities of auto port forwarding with UPnP

- **Lack of user awareness**: most users are unaware when UPnP opens ports on their routers. This automatic behaviour can lead to unintentional exposure of network services to the internet. Users often do not realize that their devices are accessible from outside their home network, increasing the risk of unauthorized access and exploitation.
- **Potential for abuse**: malware or malicious applications can exploit UPnP to open ports without user consent, creating a direct pathway into the network. This makes it easier for attackers to conduct activities such as installing botnets, launching attacks, or stealing data. The lack of robust authentication in UPnP exacerbates this risk, as any device on the local network can potentially interact with the router.
- **Default enablement risk**: UPnP is frequently enabled by default on many routers and IoT devices. This default setting means that even users who are unaware of UPnP or its implications are exposed to its risks. Default enablement can lead to situations where multiple devices independently open ports, creating a complex and potentially insecure network environment without the user's knowledge or intervention.

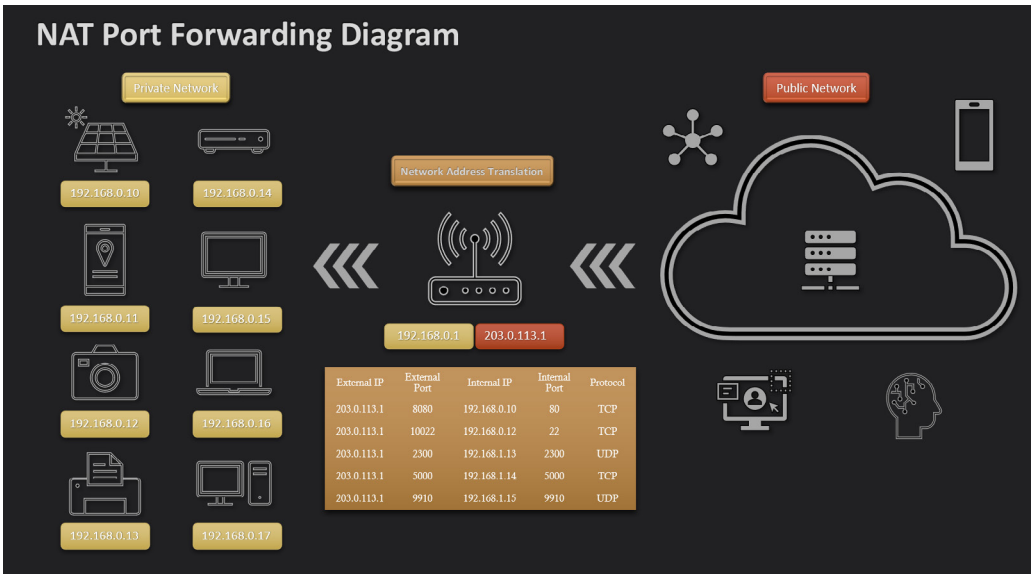

Figure 5: Illustration showing a typical household router NAT table.

UPnP CONFIGURATIONS IN ROUTERS: A REAL-WORLD ANALYSIS

It is commonly believed that UPnP is frequently enabled by default on routers provided by internet service providers (ISPs) or purchased directly from manufacturers. This belief is supported largely by anecdotal evidence from users and security professionals who regularly encounter this configuration in the field. However, there is a surprising lack of comprehensive data available on the internet to substantiate these claims. To address this gap, we undertook a two-pronged approach to gather real-world data on UPnP configurations: a user questionnaire distributed via social networks and an analysis of extracted firmware configurations from routers provided by ISPs, primarily in Europe.

UPnP questionnaire results

We conducted a survey across social networks, receiving responses from several individuals about their routers' UPnP settings. The survey focused on two main questions:

Was UPnP or NAT-PMP enabled in factory default settings?

- 43% responded No.
- 33% responded I don't know.
- 24% responded Yes.

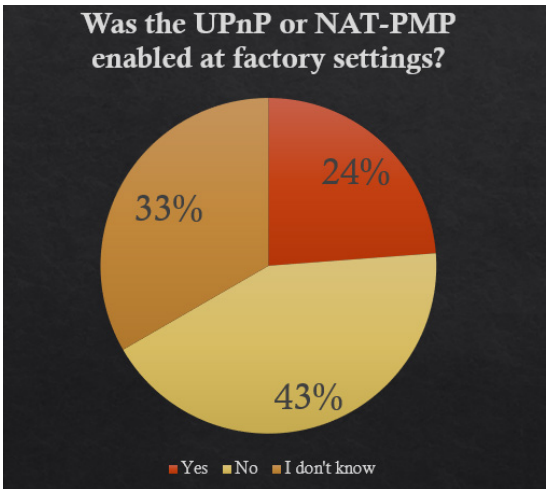

Figure 6: Response to 'Was UPnP or NAT-PMP enabled at factory default settings?'.

These results indicate a significant portion of users are either unsure or find UPnP not enabled by default, challenging the assumption that it is always turned on out-of-the-box. However, the considerable 'I don't know' responses suggest a general lack of awareness about these settings among users.

Did you modify the default state of UPnP or NAT-PMP?

- 90% responded No.
- 10% responded Yes.

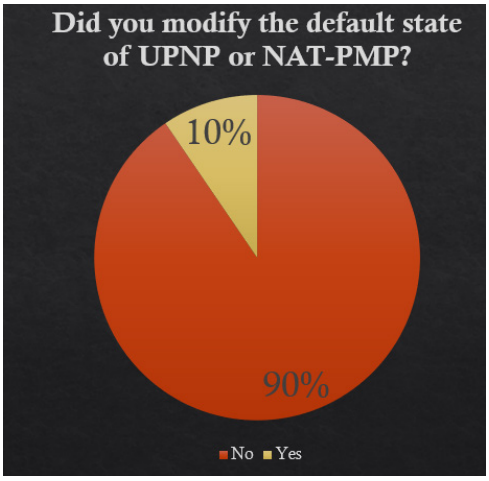

Figure 7: Response to 'Did you modify the default state of UPnP or NAT-PMP?'.

This second set of responses reveals that most users do not alter the default UPnP settings, whether they are aware of them or not. This lack of modification underscores the potential risk posed by default settings, as users typically leave them unchanged.

It's important to note that the respondents to this questionnaire likely have a higher level of technical expertise, which may influence their awareness and understanding of UPnP settings.

Analysis of extracted UPnP configurations

To complement the questionnaire, we analysed the firmware of routers that are supplied by ISPs, focusing on *Technicolor* models (mainly European models) that are based on the openWRT platform. This analysis aimed to determine the default state of UPnP in these devices.

UPnP configuration distribution:

- 88% had UPnP enabled.
- 9% had UPnP disabled.
- 3% had UPnP enabled with secure mode disabled.

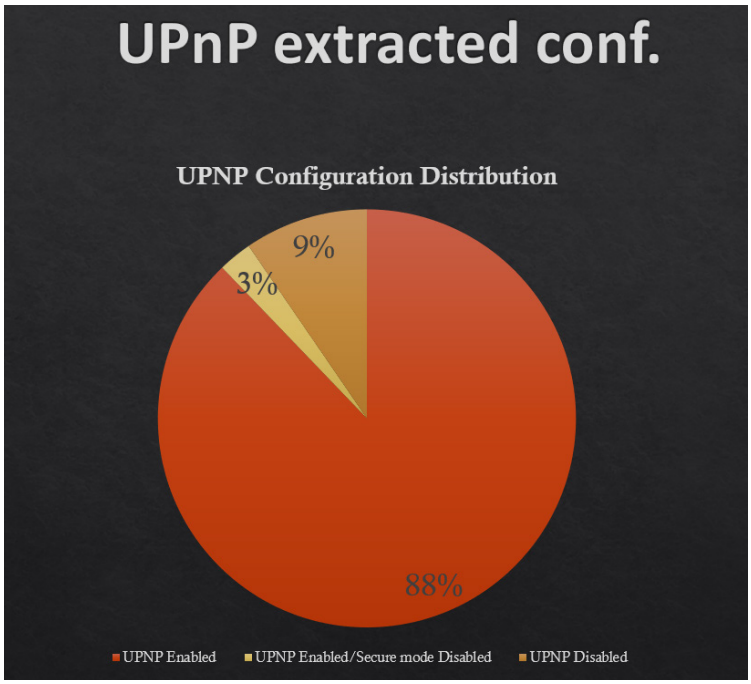

Figure 8: UPnP configuration distribution.

These findings confirm that most routers analysed had UPnP enabled by default. The small percentage with secure mode disabled further emphasizes the potential security risks, as this mode is designed to add an extra layer of protection.

Challenges in firmware analysis

Analysing firmware for UPnP settings is complex due to the varied ways these configurations are implemented across different ISPs and device models. The following are the common locations and methods where these settings are found:

- **UCI config source files**: typically found in /etc/config/* , to highlight /etc/config/upnpd for the UPnP daemon settings and /etc/config/firewall for related firewall rules.
- **Services and initialization script**: scripts in /etc/init.d/ directory, such as /etc/init.d/upnpd, may dynamically set UPnP parameters during the router's startup.
- **Executables, and many custom-written scripts for this hardware**: many ISPs use proprietary scripts in directories like /sbin/*.sh, /usr/bin/*.sh, /usr/sbin/*.sh, which can override or adjust UPnP settings post-setup or during updates.
- **Embedded system scripts**: some configurations are hard coded in scripts that run during the router's first boot or after a factory reset, often found in /etc/rc.local.
- **Lua/HTML web interface source files**: the web interface location /www/* might contain additional scripts to customize the device settings.

Conclusion

Though this was not a comprehensive analysis significant for the global internet population, it supports the assessment that UPnP is often enabled by default on household routers, posing significant security risks. Additionally, it highlights the general lack of user awareness about this setting and what it means.

RECENT UPnP FAIL: THE LG webOS TV VULNERABILITIES

UPnP's ease of use can sometimes lead to serious security oversights, as seen in the recent vulnerabilities affecting *LG*'s *webOS* TVs. These vulnerabilities highlight how a seemingly benign feature intended for local network control can become a significant risk when combined with aggressive UPnP behaviour and routers that have UPnP enabled by default.

The issue

LG's *webOS* TVs include a remote control feature through the *ThinkQ Smart* application, which operates over ports 3000 and 3001. This functionality is designed for use within the local network, allowing users to manage their TVs from their smartphones or other devices without complex setups. However, this feature, when coupled with UPnP's automatic port forwarding, created a pathway for broader exposure and exploitation.

Vulnerabilities exploited

Several critical vulnerabilities were discovered in *LG*'s *webOS* TVs that could be exploited through these open ports:

- **CVE-2023-6317**: this vulnerability allows attackers to add an unauthorized user to the TV without proper authentication by exploiting a flaw in the TV's authorization mechanism.
- **CVE-2023-6318**: once unauthorized access is gained via CVE-2023-6317, attackers can elevate their privileges to gain root access, the highest level of control on the device.
- **CVE-2023-6319**: this involves a command injection vulnerability, enabling attackers to execute arbitrary commands on the TV by manipulating a library used for displaying music lyrics.
- **CVE-2023-6320**: this vulnerability allows authenticated command execution as the dbus user, which has permissions like those of the root user, providing significant control over the device.

The role of UPnP

UPnP played a critical role in exposing these vulnerabilities:

- **Aggressive UPnP requests**: the *LG* TVs, upon installation, aggressively requested port forwarding through UPnP to facilitate remote control functionalities intended for local network use.
- **Edge routers with UPnP enabled**: many routers, with UPnP enabled by default, automatically honoured these requests, opening ports 3000 and 3001 to the internet without user knowledge or intervention.
- **Wider exposure**: this automatic opening of ports exposed the TVs to the internet, making them vulnerable to remote attacks from anywhere, not just within the local network as originally intended.

A *Shodan* search (a tool that maps devices connected to the internet) revealed that over 90,000 *LG* smart TVs were potentially exposed and vulnerable to these exploits. This widespread exposure underscores the risks associated with having UPnP enabled by default, as it can lead to unintended and potentially dangerous network configurations.

The *LG webOS* TV vulnerabilities illustrate a significant failure where UPnP's convenience turned into a serious security liability. The combination of aggressive UPnP behaviour by devices and default-enabled UPnP settings on routers resulted in a large population of devices being exposed to the internet.

ALTERNATIVES AND SOLUTIONS TO UPnP AUTO PORT FORWARDING

To mitigate some of the risks we have mentioned to this point, several more secure alternatives and measures should be considered. In the following we outline three practical steps that can improve network security by addressing the vulnerabilities associated with UPnP.

Implementing UUID cloud access solutions

One alternative to direct port forwarding through UPnP is utilizing a UUID (Universally Unique Identifier) cloud access solution. In this model, devices do not directly open ports on the edge router. Instead, they establish outbound connections to a secure cloud service, which then facilitates the necessary communication. This method has several advantages:

- **No open ports**: since the connection is initiated by the device to the cloud, no ports need to be opened on the router, significantly reducing the attack surface.

- **Secure, managed access**: cloud services can manage and monitor these connections, providing an additional layer of security and potentially identifying and mitigating suspicious activities.
- **Simplified network configuration**: Users benefit from easy setup without compromising security, as they don't need to understand or manage complex port forwarding rules.

While this approach does have its challenges – such as dependency on the cloud provider and potential privacy concerns – it offers a safer alternative to UPnP's automatic port forwarding.

Clear disclaimers and warnings in router configuration

Users typically have no idea what the UPnP setting does or its implications, and the router configuration interfaces do little to explain the severity of this setting, as shown in Figures 9 and 10.

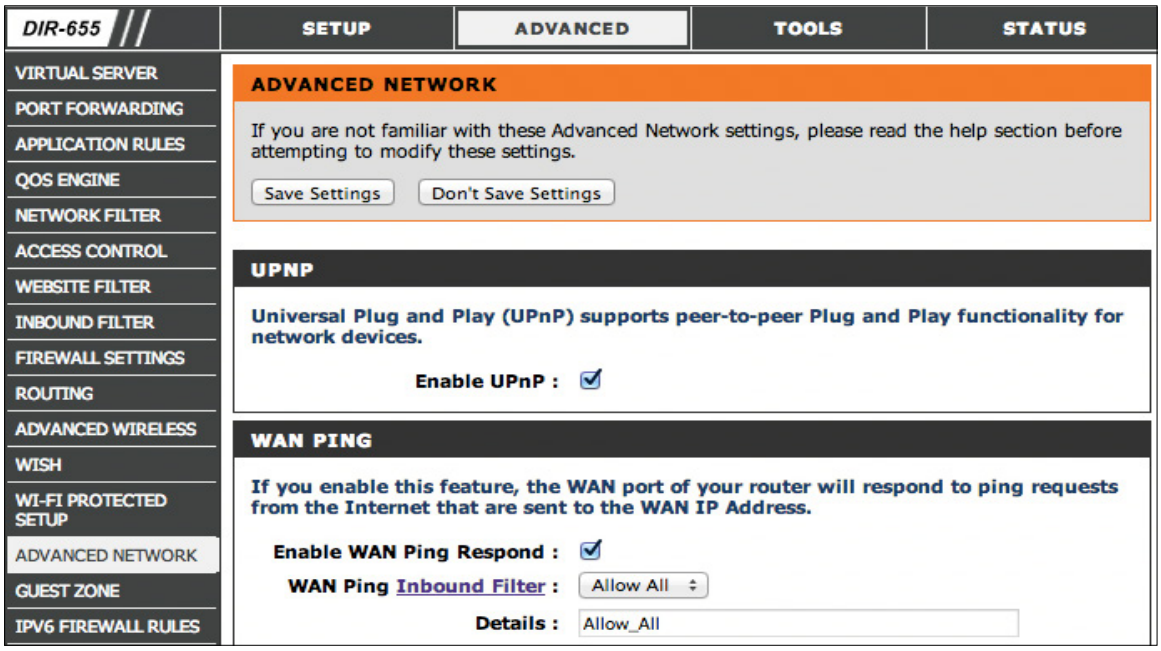

Figure 9: D-Link configuration page.

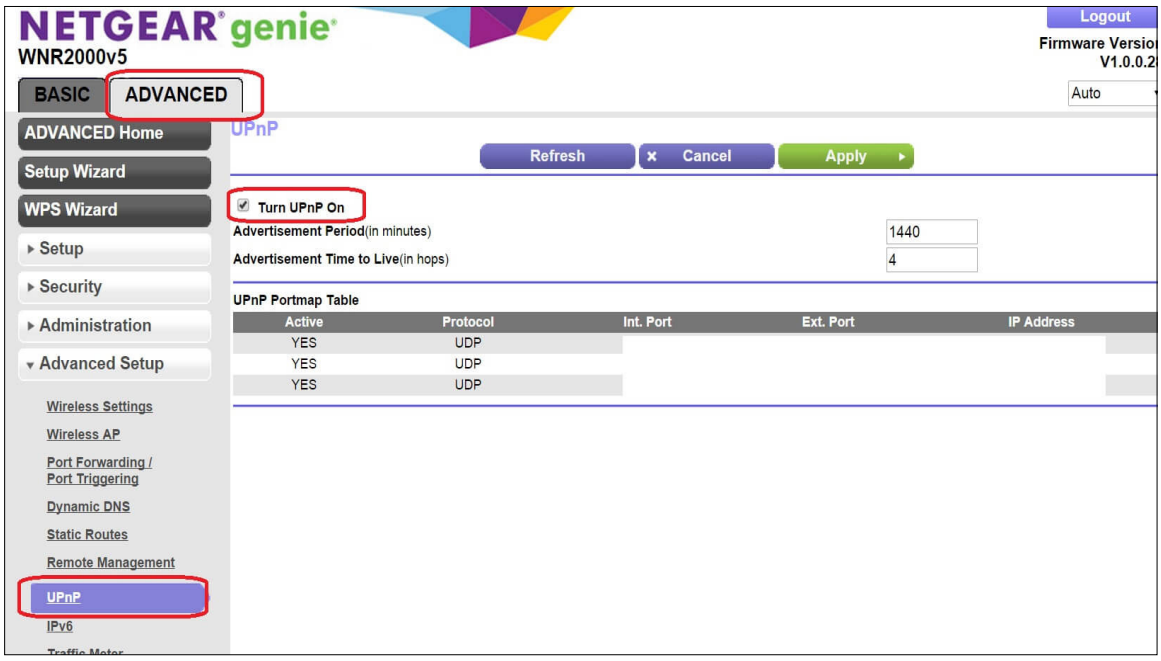

Figure 10: Netgear configuration page .

To address this, routers should include explicit disclaimers and warnings about UPnP settings in their configuration interfaces. This would help users make informed decisions about their network security.

For example, Figure 11 shows a proposed warning message.

Figure 11: Proposed warning message.

Including such messages would increase user awareness and help them understand the potential security implications of enabling UPnP.

Disable UPnP by default

At the very least, UPnP should be disabled by default on all routers. Users should be required to consciously enable this feature if they need it, making them more aware of the associated risks. This approach has several benefits:

- **Enhanced security**: with UPnP disabled by default, the network is less likely to be exposed to unauthorized remote access and other security threats.
- **User awareness**: requiring users to manually enable UPnP means they are more likely to be aware of the feature and consider whether they need it, promoting better security practices.
- **Reduced risk of exploitation**: disabling UPnP by default prevents devices from automatically opening ports, reducing the chances of vulnerabilities being exploited by malicious actors.

FINAL THOUGHTS

The discussion around UPnP and its security implications is part of a broader debate in the field of IT about the balance between convenience and security. As technology continues to evolve, this tension becomes increasingly pronounced, particularly in complex IT environments.

Convenience vs security

The issue with UPnP is emblematic of a larger problem in IT: choosing between ease of use and robust security. UPnP's automatic port forwarding offers undeniable convenience, simplifying network setup and device connectivity for users who may not have technical expertise. However, this simplicity often comes at the cost of security, exposing networks to potential threats. This trade-off is a common theme in IT, where solutions that are easy to implement and use can inadvertently introduce significant vulnerabilities. As IT professionals and users, it is crucial to be mindful of these trade-offs and prioritize security where possible, especially as our reliance on interconnected devices grows.

The importance of user education

Like many areas of IT security, educating users is essential to mitigating risks associated with UPnP and other technologies. Users must understand that their home network is a critical part of their digital life, much like their physical home. It's not just about connecting devices; it's about securing their digital environment against unauthorized access and attacks. Raising awareness about how UPnP works and the potential risks of leaving it enabled by default can empower users to make informed decisions. Education can bridge the gap between convenience and security, helping users to protect their 'invisible' digital home as diligently as their physical ones.

Future technologies and security implications

As we look to the future, the landscape of network connectivity and device interaction is set to become even more complex with the advent of technologies like IPv6, Matter, Thread, and 5G.

- **IPv6**: with a vastly larger address space than IPv4, IPv6 enables direct device-to-device communication across the internet, eliminating the need for NAT (Network Address Translation). This could simplify network configurations but also poses new security challenges, as every device is potentially accessible globally.
- **Matter and Thread**: these protocols are designed to enhance interoperability and simplify the setup and operation of smart home devices. While they promise greater ease of use, they also need robust security measures to protect against unauthorized access and control.
- **5G**: the rollout of 5G networks promises faster speeds and more reliable connections, enabling a new generation of connected devices and services. However, this increased connectivity also expands the attack surface, necessitating more advanced security strategies to protect users and their data.

In conclusion, as technology continues to advance, balancing convenience and security remains a fundamental challenge. By prioritizing user education and implementing secure alternatives to potentially vulnerable configurations like UPnP, we can better safeguard our networks against future threats. As the digital and physical worlds converge, it's more important than ever to stay informed and proactive in protecting our interconnected lives.