Open by Default

The Hidden Cost of Convenience in Network Security

By Aurelio Picón López

CUJOAI

ABOUT ME

Large Corporate Network Experience: Expertise in risk analysis and threat hunting for big corporations.

Data Insights: Access to anonymized user security data.

IoT Security Focus: Designing for IoT protection.

Botnet Expertise: Detecting and analyzing botnet malware.

Insight into Threat Actors

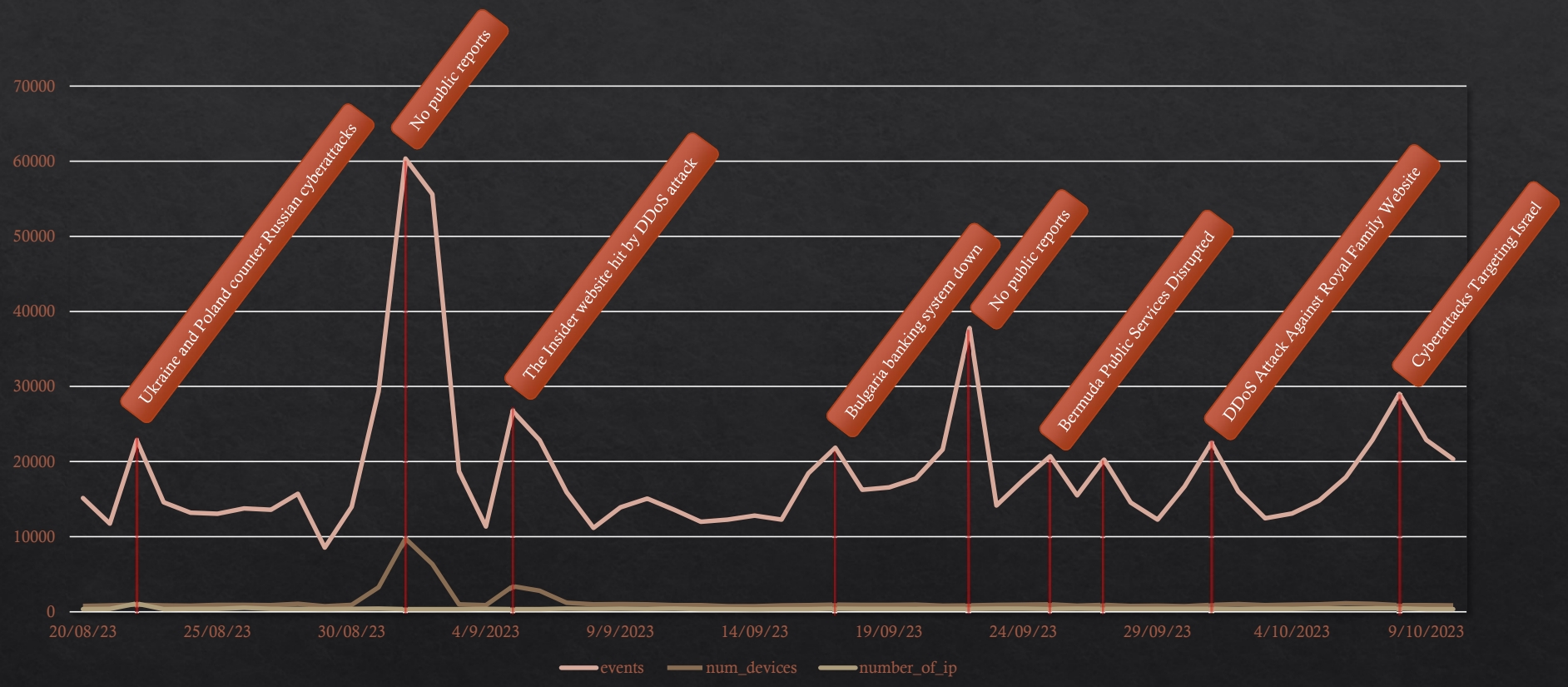
and Targeted Devices

Case Study: KillNet

"KILLNET will launch powerful attacks on European and American enterprises, which will indirectly lead to casualties"

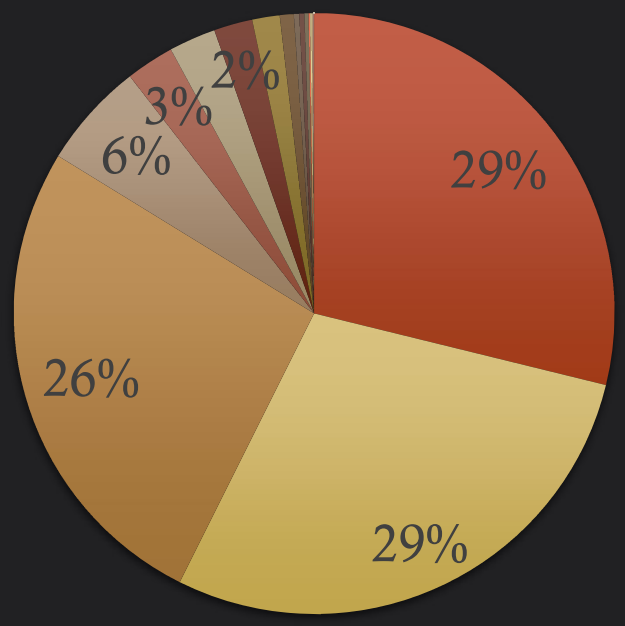
~KillMilk

KILLNET: Progression of events



CUJOAI

TOP Remote Accessed IOT devices

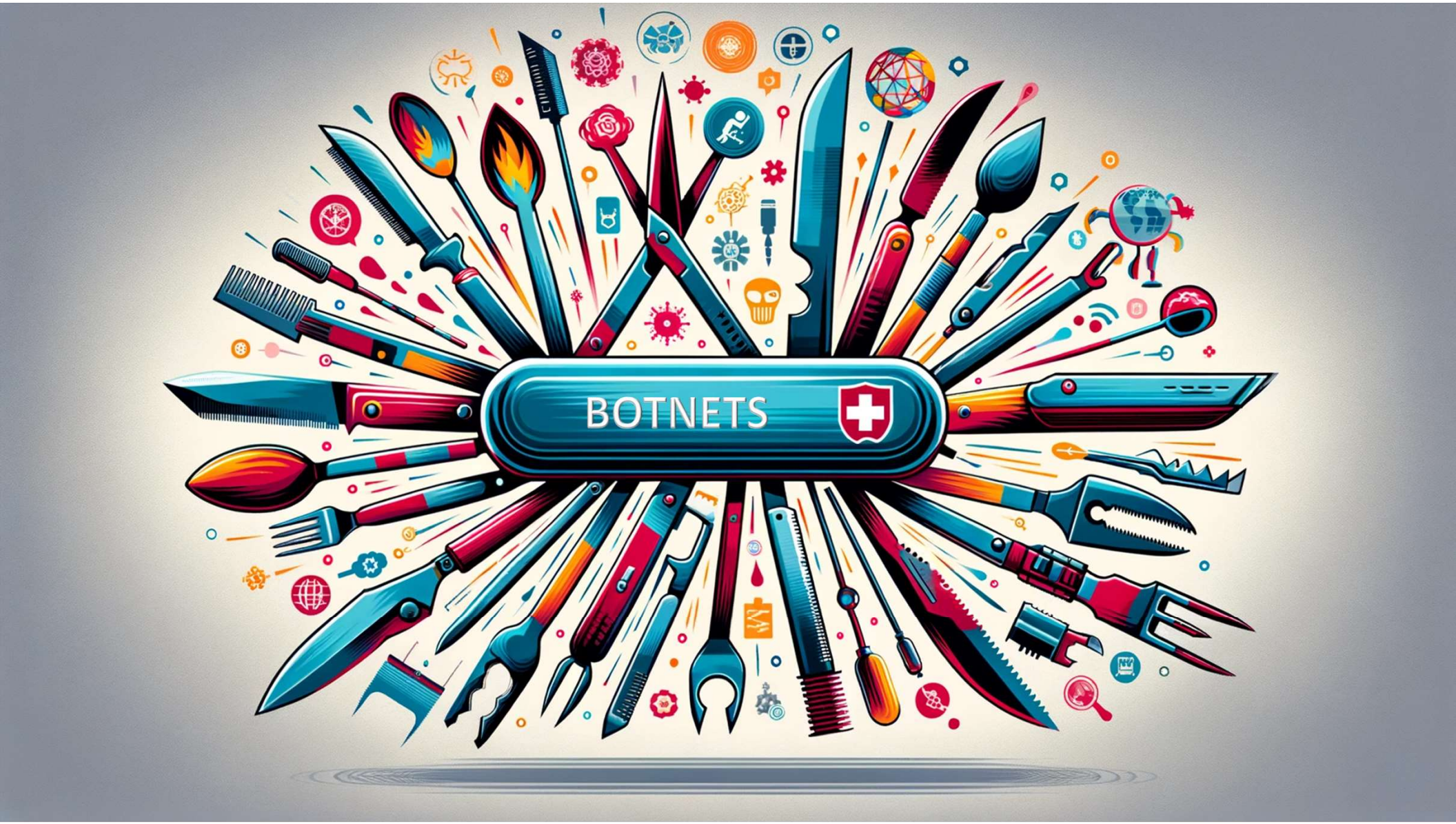


- Set-Top Box
- Router
- Generic device
- NAS Storage
- Other Network Deivce
- IP Camera
- Camera
- Other
- DVR
- Smart TV
- Audio-Video Device
- Wi Fi Access Point
- IoT Device
- Other Device
- Car

CUJOAI

Compromised Devices

Threat Actors Swiss Army Knife


BOTNETS

- Distributed Denial-of-Service (DDoS)
- Proxy Networks
- Cryptocurrency Mining
- Email Spam Campaigns
- Ransomware and Malware Distribution
- Surveillance and Espionage
- Data Theft
- Network Infiltration
- Credential Stuffing
- Ad Fraud
- Identity Spoofing
- Manipulating Physical Systems

The Core Problem

UPnP and Security

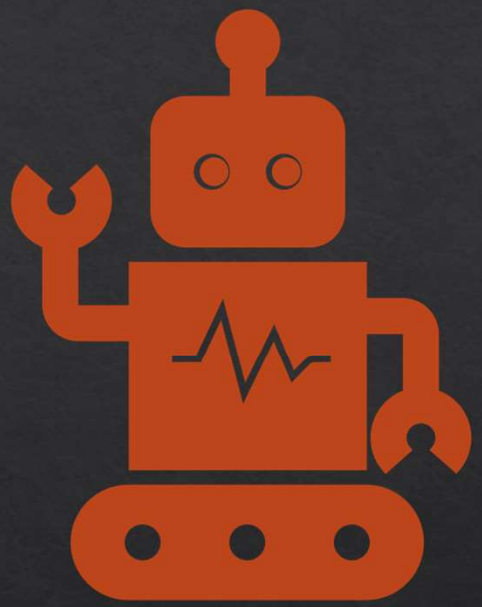
Universal Plug and Play (UPnP)

Automatic Discovery:

UPnP enables devices on a local network to discover and communicate with each other without manual configuration.

Device Interoperability:

It simplifies connecting printers, game consoles, routers, and other devices seamlessly.



UPNP vulnerabilities

Lack of Authentication

Poor Input Validation

Memory Corruption Bugs

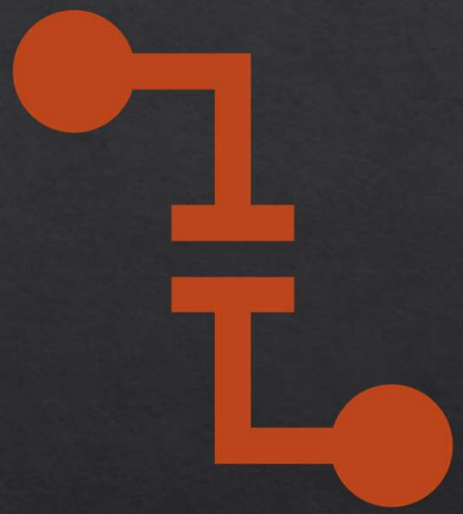
SQL Injection

XML External Entity (XXE) Attacks

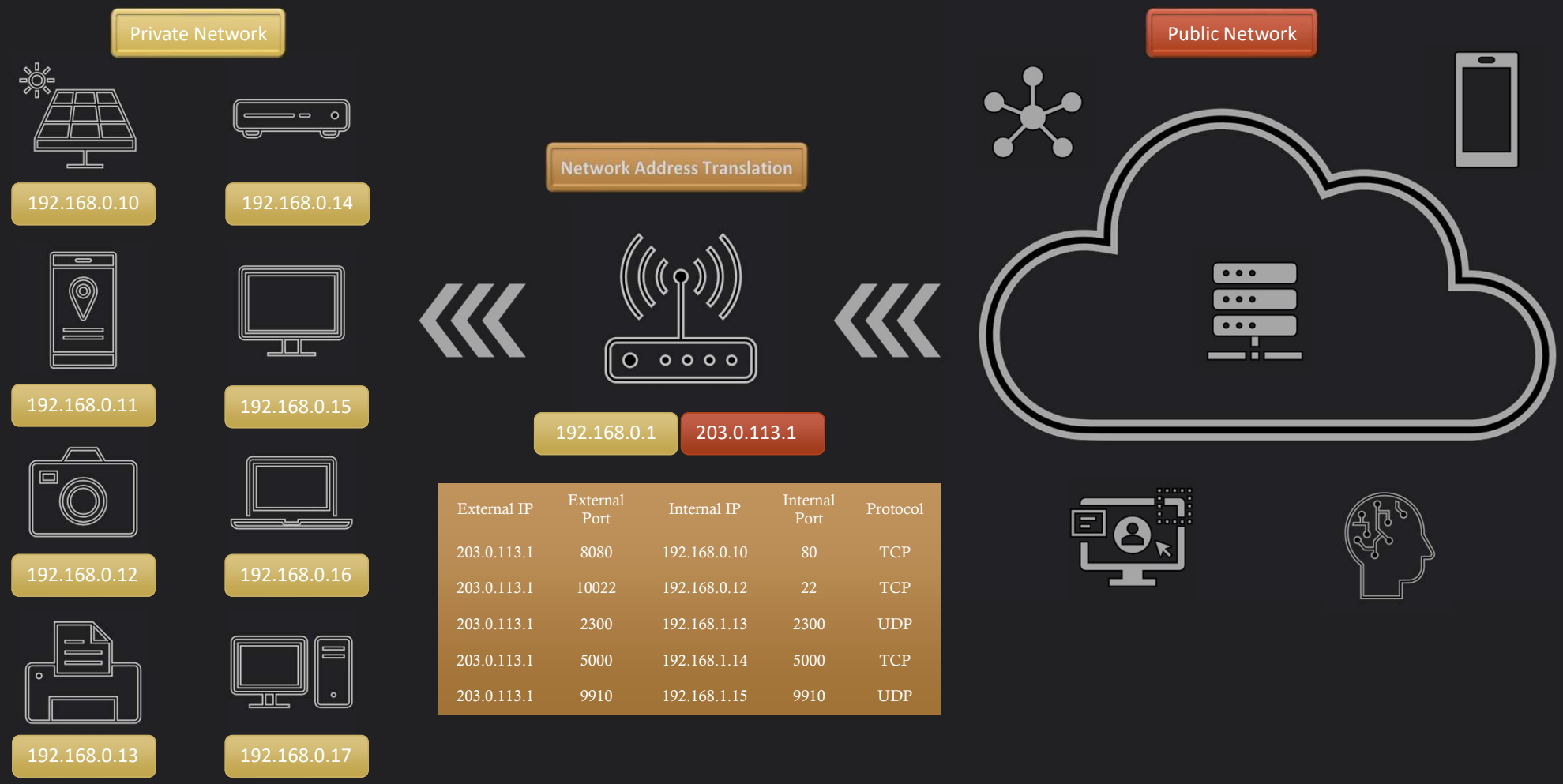
Exposure to WAN Requests

Lack of Logging

Insecure IGD Protocol Implementation



NAT Port Forwarding Diagram



External IP	External Port	Internal IP	Internal Port	Protocol
203.0.113.1	8080	192.168.0.10	80	TCP
203.0.113.1	10022	192.168.0.12	22	TCP
203.0.113.1	2300	192.168.1.13	2300	UDP
203.0.113.1	5000	192.168.1.14	5000	TCP
203.0.113.1	9910	192.168.1.15	9910	UDP

Auto Port Forwarding with UPnP

AUTOMATIC CONFIGURATION

DYNAMIC RESPONSE TO DEVICES

TEMPORARY OPEN PORTS

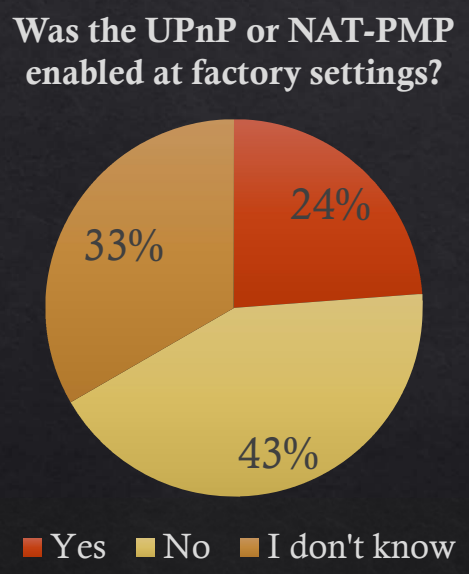
Auto Port Forwarding with UPnP

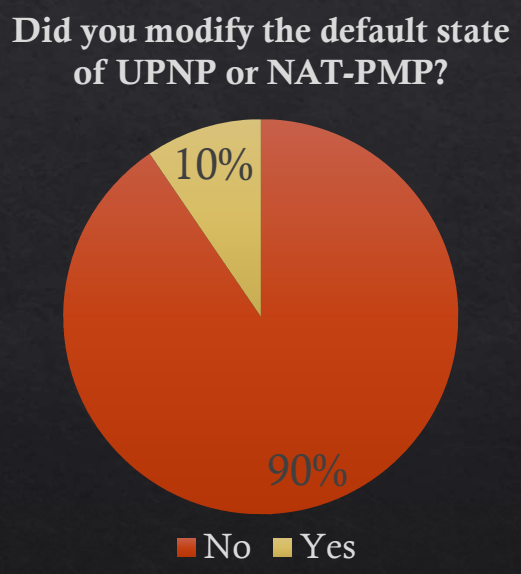
LACK OF USER AWARENESS

POTENTIAL FOR ABUSE

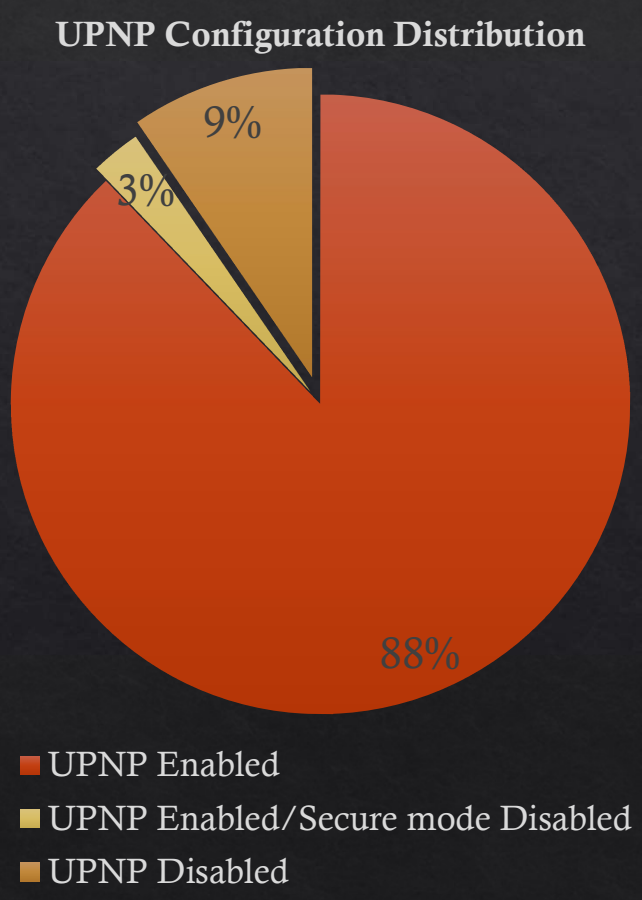
DEFAULT ENABLEMENT RISKS

UPnP Questionnaire

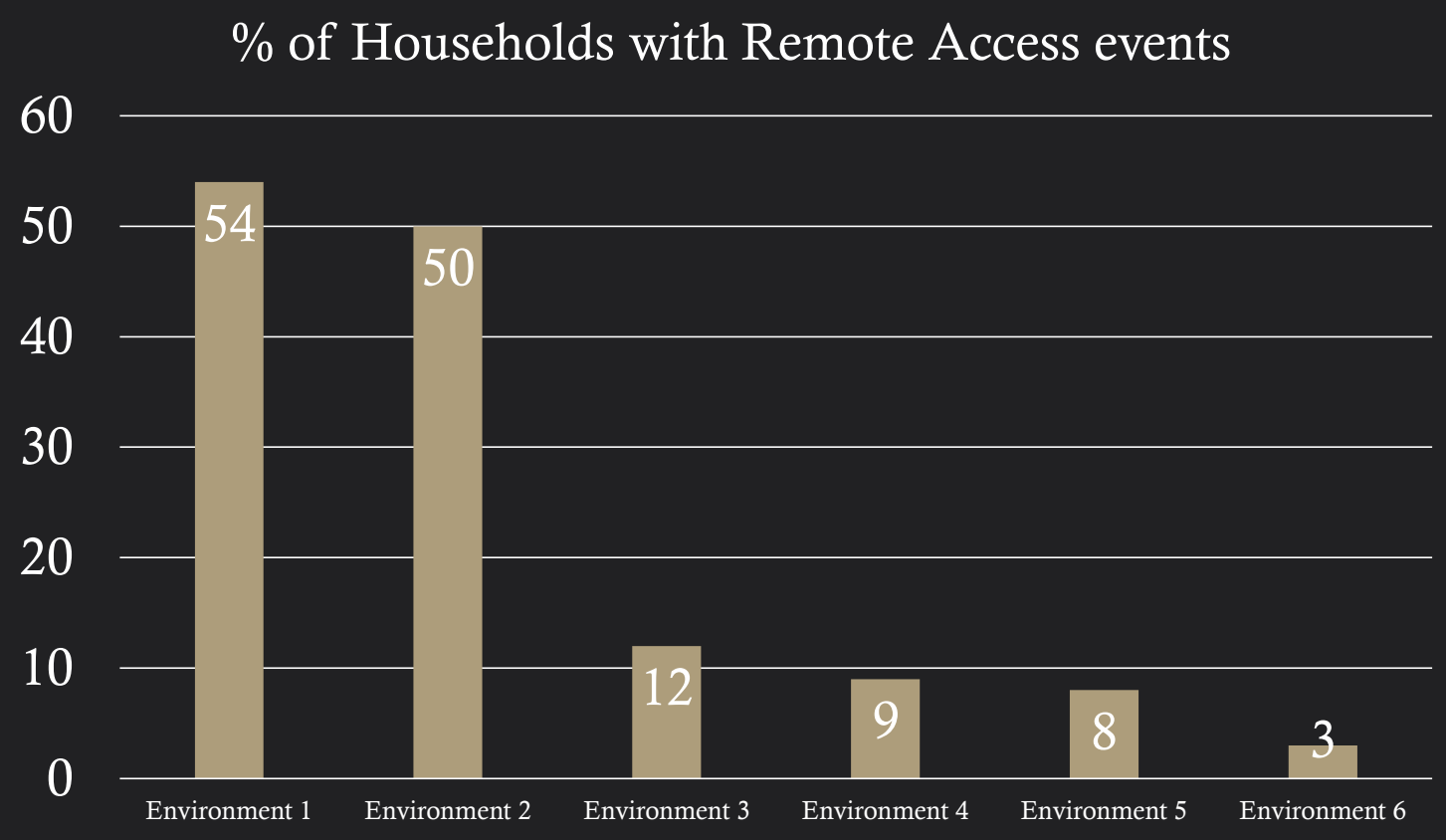




UPnP extracted conf.

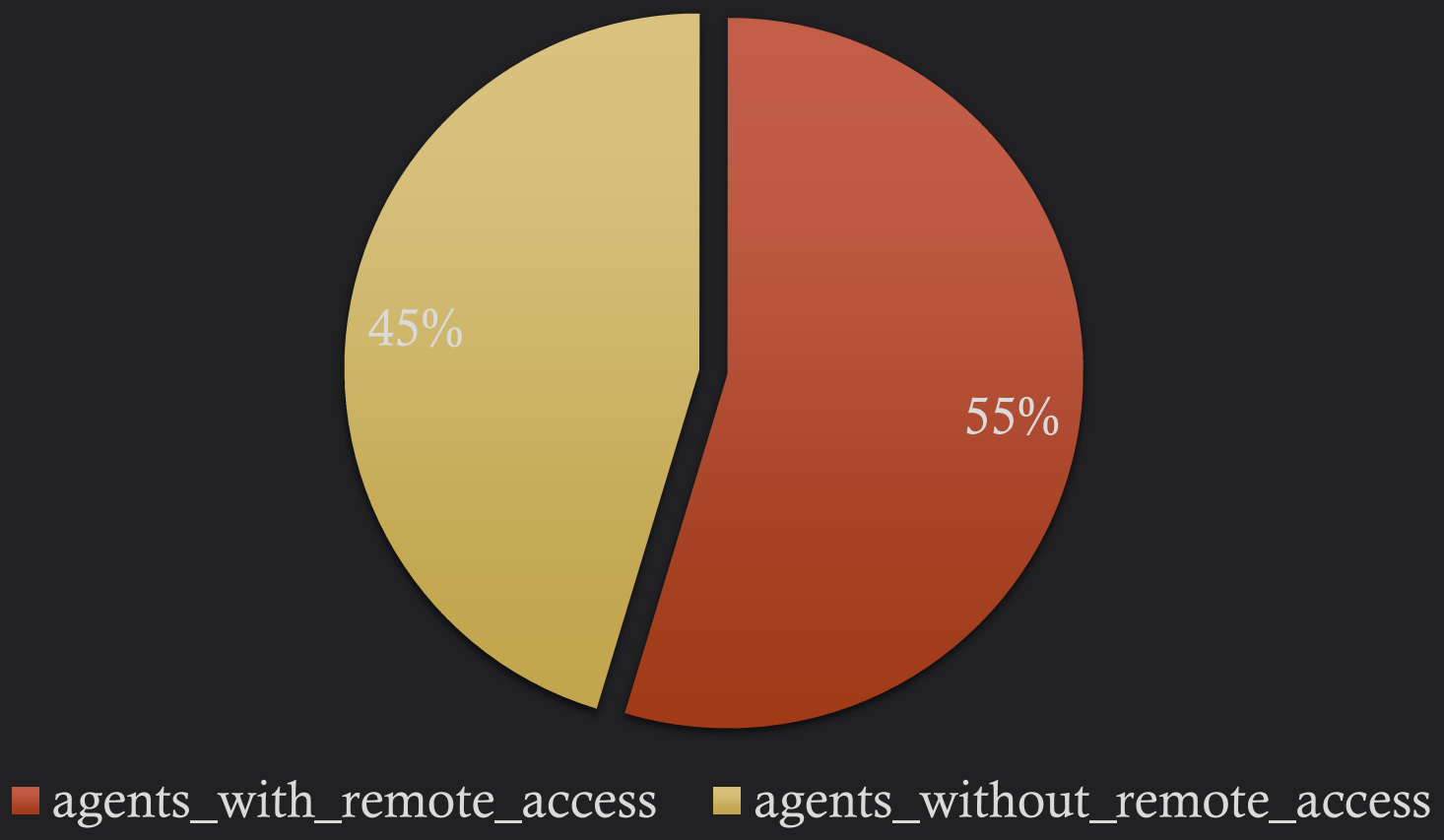


Remote Access Events Distribution



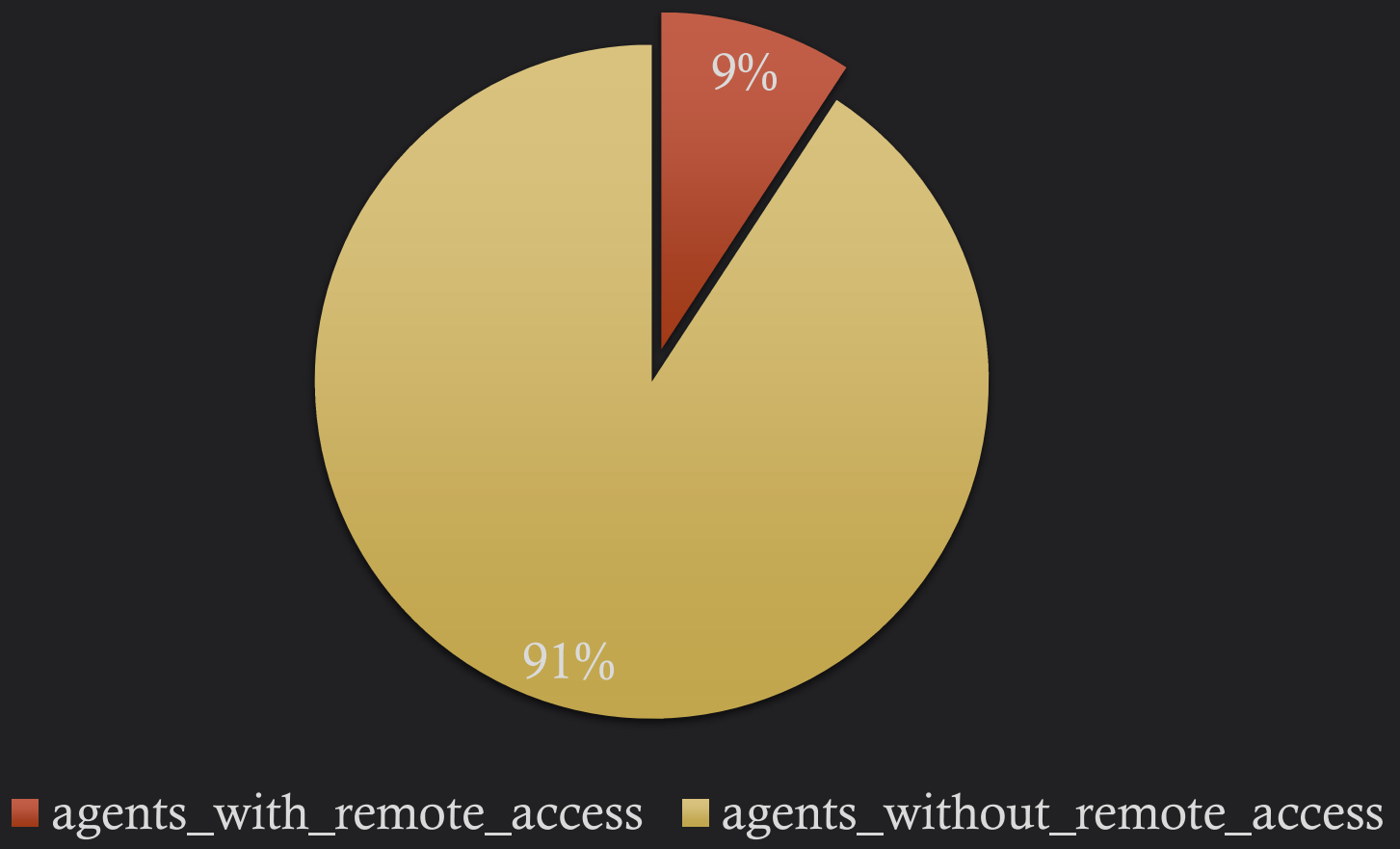
CUJOAI

UPNP Enabled by Default



CUJOAI

UPNP Disabled by Default



CUJOAI

Recent UPNP FAIL

- **LG webOS TV Vulnerabilities**

  CVE-2023-6317 allows attackers to the addition of an extra user to the TV set without proper authorization.

  CVE-2023-6318 allows attackers to gain root access

  CVE-2023-6319 allows execution of local arbitrary commands.

  CVE-2023-6320 enables command execution as the dbus user

- **Exploitation through UPnP**:

  LG TVs utilize the ThinkQ Smart application, communicating over ports 3000 and 3001 for remote control functionalities intended for local LAN use.

  Aggressive UPNP request port forwarding on edge routers to facilitate this communication on adjacent networks.

  UPnP-enabled edge routers automatically open these ports, exposing the vulnerable devices to the internet.

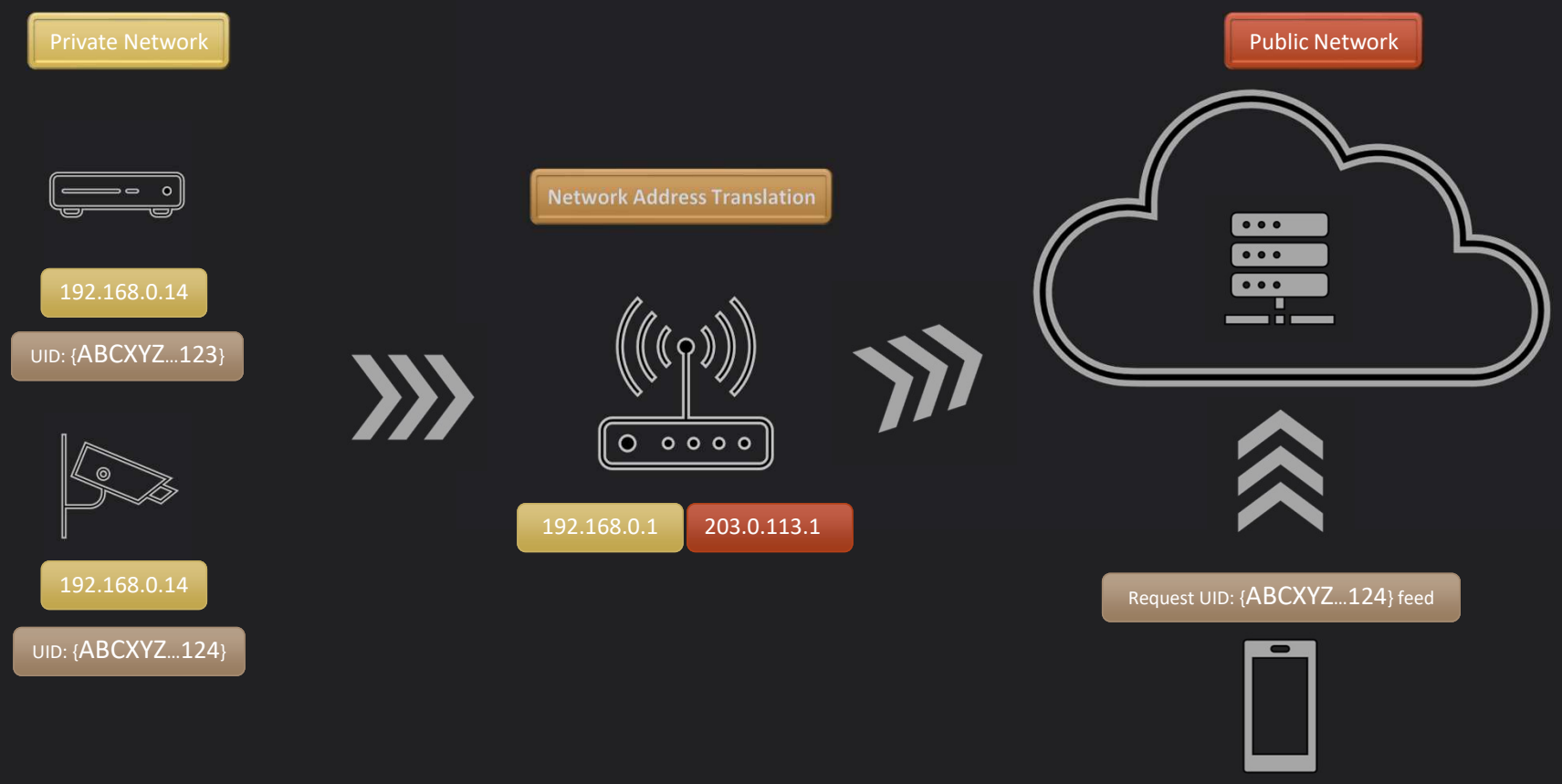
  SHODAN search shows 90k~ possible targets.

Alternatives and Solutions

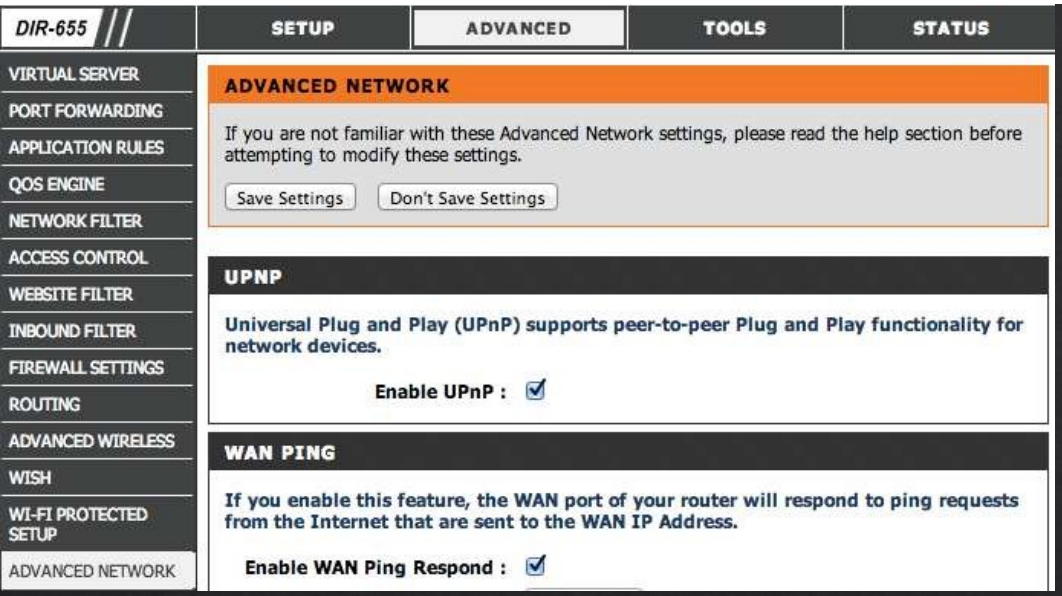
and Responsibilities

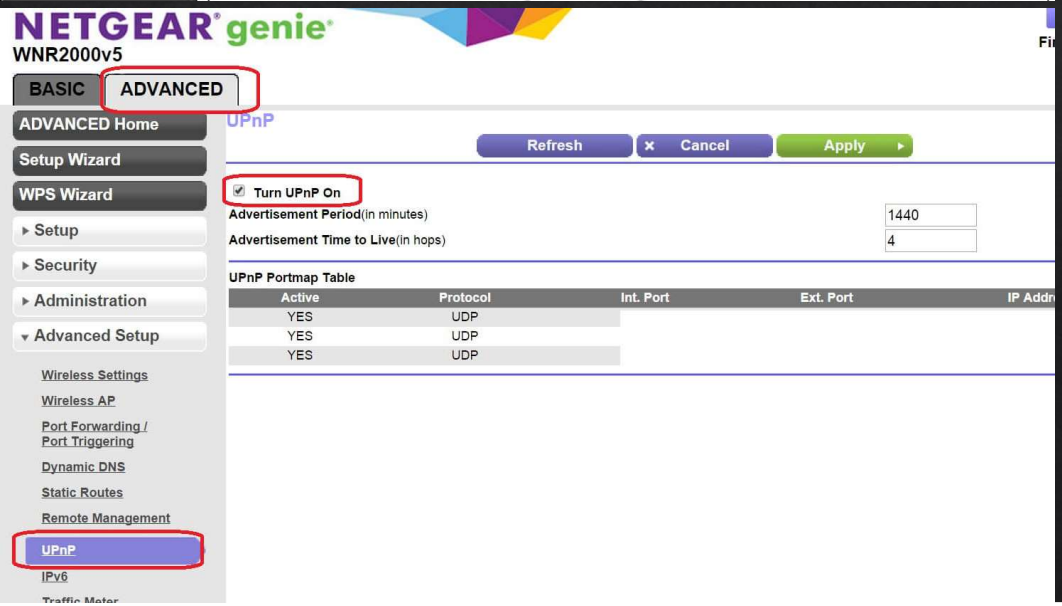
Cloud-Based Solutions for Accessibility

Ex. UUID Cloud Access



UPnP Activated by Default





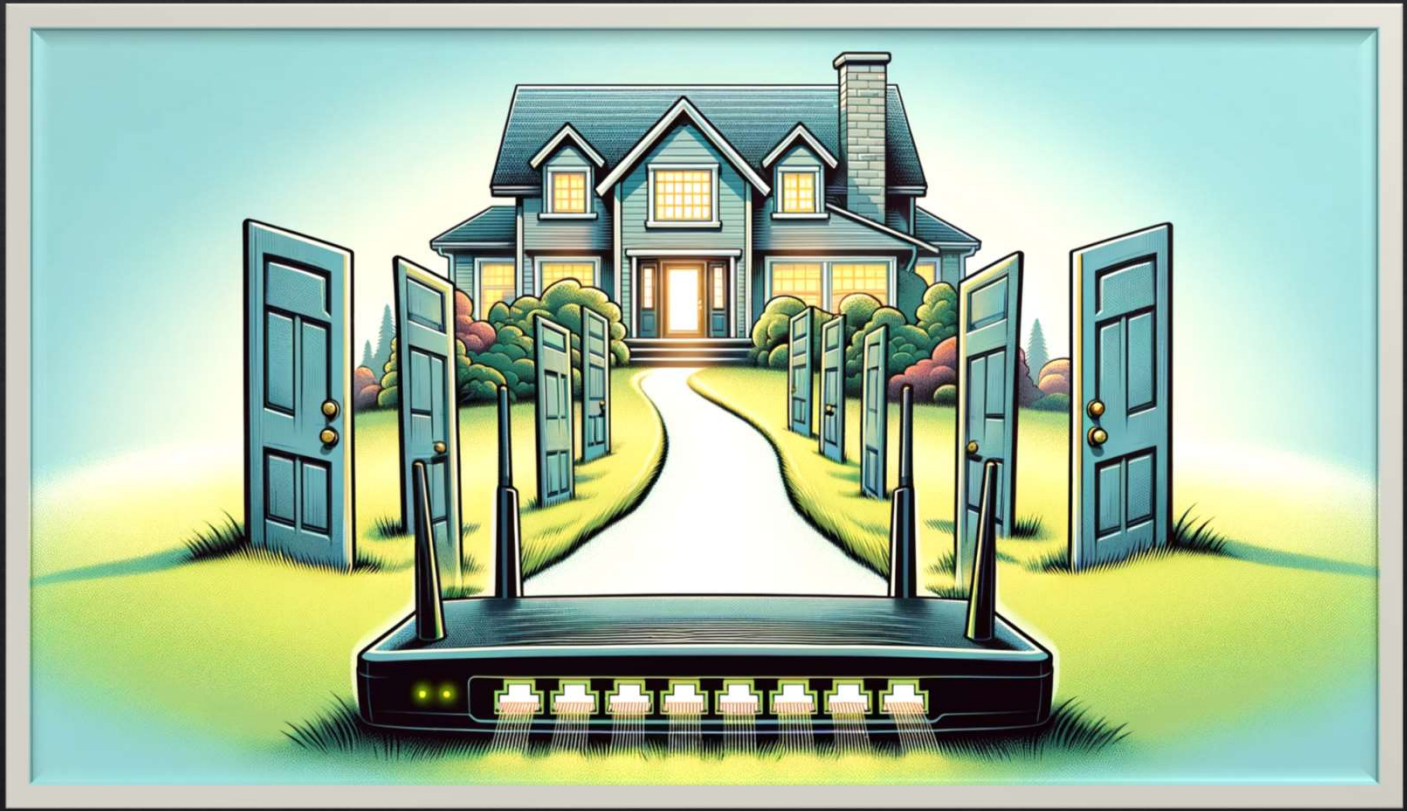
Clear Disclaimers and Warnings When Activated

- **Attention:**

  You are about to enable Universal Plug and Play (UPnP) on your device. While UPnP provides convenience by automatically setting up port forwarding for your devices, it may expose your network to external threats.

- **Proceed with Caution:**
  - UPnP can be exploited by malicious actors to open ports without your knowledge, making your network accessible from the internet.
  - If a device on your network is compromised, UPnP may allow the spread of malware or unauthorized access to other devices.
  - We strongly recommend using UPnP only if you understand the risks and it is absolutely necessary.
- **Recommendations:**
  - Consider manual port forwarding configuration.
  - Ensure all your devices are updated with the latest security patches.
- **By activating UPnP, you acknowledge the potential risks and agree to proceed at your own risk.**

Abandoning Automated Port Forwarding



Convenience VS Security

A more general problem

The Trade-Off

Example of Poor Security Advice

Microsoft | XBOX Support home Xbox status Help topics Accessible gaming Xbox system updates

Home > **Hardware & networking**

"UPnP Not Successful" appears in your network settings

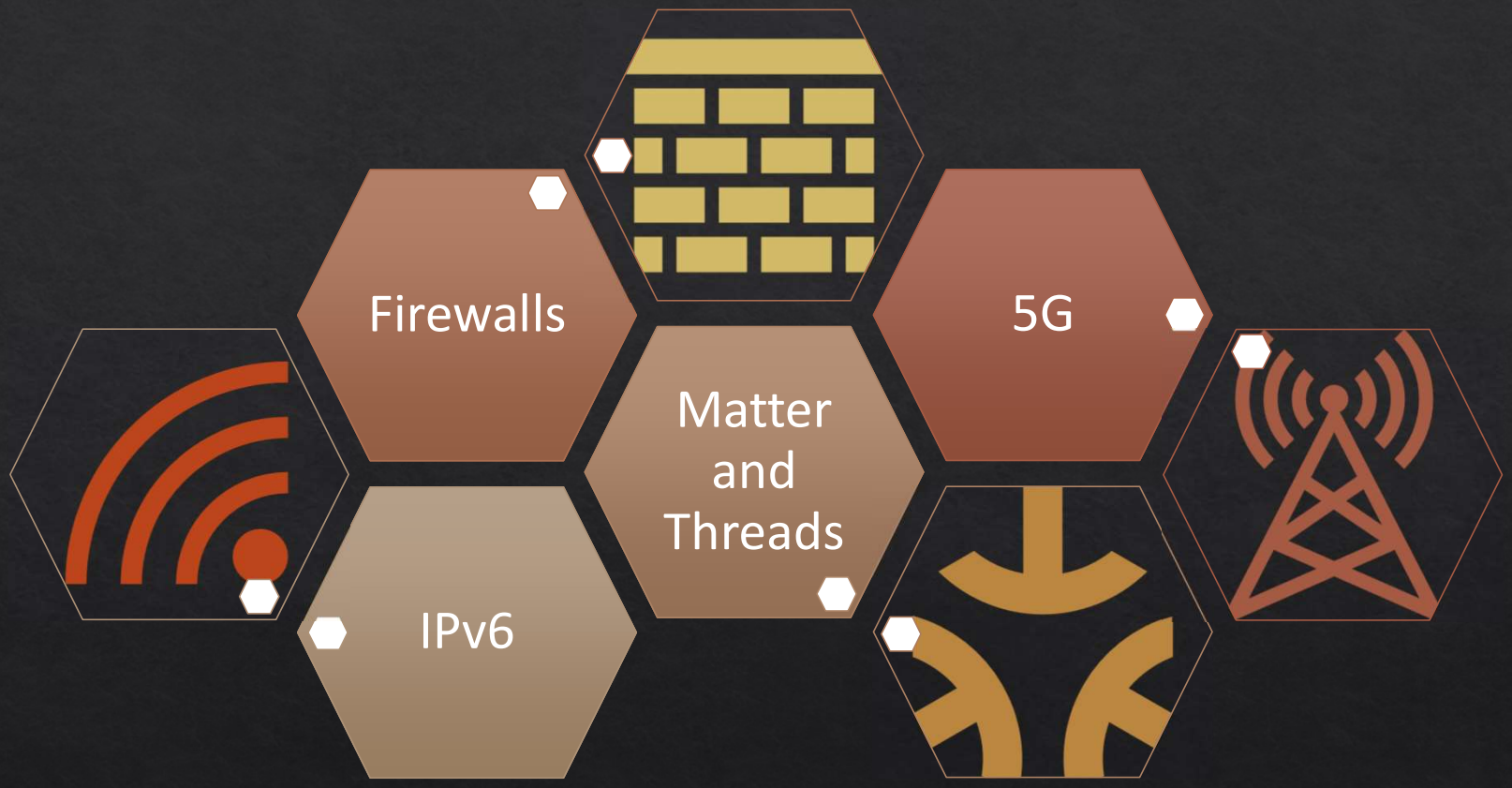
Universal Plug and Play (UPnP) is what your Xbox uses to set up your router for multiplayer gaming and chat. If you see "UPnP Not Successful" in your console's **Network settings**, first see if your router needs an update. If your router has the latest manufacturer update:

1. Sign in to your router's setup webpage, and make sure the router's UPnP setting is turned on. You can usually find first-time help with this in the router manual or on the manufacturer's support site.
2. Turn the UPnP setting off and save your changes.
3. Restart your console, your modem, and your router.
4. Turn the UPnP setting back on and save your changes. If there's a Zero Config setting, make sure that's turned on as well.
5. Restart your modem and router.

Understanding the Consequences

The Future

Changing landscape


Firewalls
5G
Matter and Threads
IPv6

Call to Action

Against Auto-Port Forwarding

- Internet is Dangerous
- Households are Coveted Resources
- Security Disabled by Default
- Convenience Over Security
- Undereducated Users
- Uncertain Future

- Don’t advise to lower security
- Clear Disclaimers and Warnings
- Running Firewall
- Alternatives for Remote Access
- No Auto Port forwarding at all
- UPnP Disabled by default

Conclusion

Future outlook


Q & A