TELEWORKING: Security for Work From Home Office Networks

IoT has created a variety of new endpoints in our home office networks that potentially expose organizational and personal data to compromise. Teleworkers have a key role in ensuring their home offices are secure from hackers and malware.

How Secure is My Home Office

What is an endpoint?

An endpoint is any device in your home that is physically connected to the network via Wi-Fi or cable. This includes all IoT devices installed on your home network including laptops, desktops, phones, tablets, printers, and other smart home devices which are considered endpoints. Compromised endpoints could breach your home and organization's network.

Why Should We Care?

1. Personal Privacy: PII, PHI, Finances, Credentials, Passports, Emails, Social Media, SMS
2. Corporate Security: PII, PHI, HR, Admin credentials, IP, Secrets/Keys/2FA/MFA, Emails, CRM, ERP
3. Malware, Ransomware, Wiperware, Cryptomining
4. Extortion/Sextortion/Robbery/Home Invasions
5. Corporate Brand and Reputational Damage

Many organizations have allowed employees to Work From Home (WFH) and some employees are using their own equipment (BYOD). This is obviously not the best security policy and requires some due diligence to ensure your work devices are not used for things like downloading apps, gaming, porn, torrents, or any other non-essential software.

IoT: How Many Are In My Home Office

SMART: phones, fridges, kettles, coffeemakers, ovens, watches, fire alarms, smoke detectors, flood sensors, door locks, scooters, bicycles, medical sensors, diabetes monitors, pacemakers, fitness trackers, security systems, doorbells, toys, Google Home, Alexa, Amazon Echo, robots, vacuums, HVAC, gun safes, thermostats, universal remote controls, baby monitors, mirrors, garage door openers, remote gates, TVs, Kodi/Roku/Firestick, light switches, AC plugs, light bulbs, weather stations, Wi-Fi extenders, storage drives, printers, irrigation systems, valves, speakers, aquariums, garden systems…

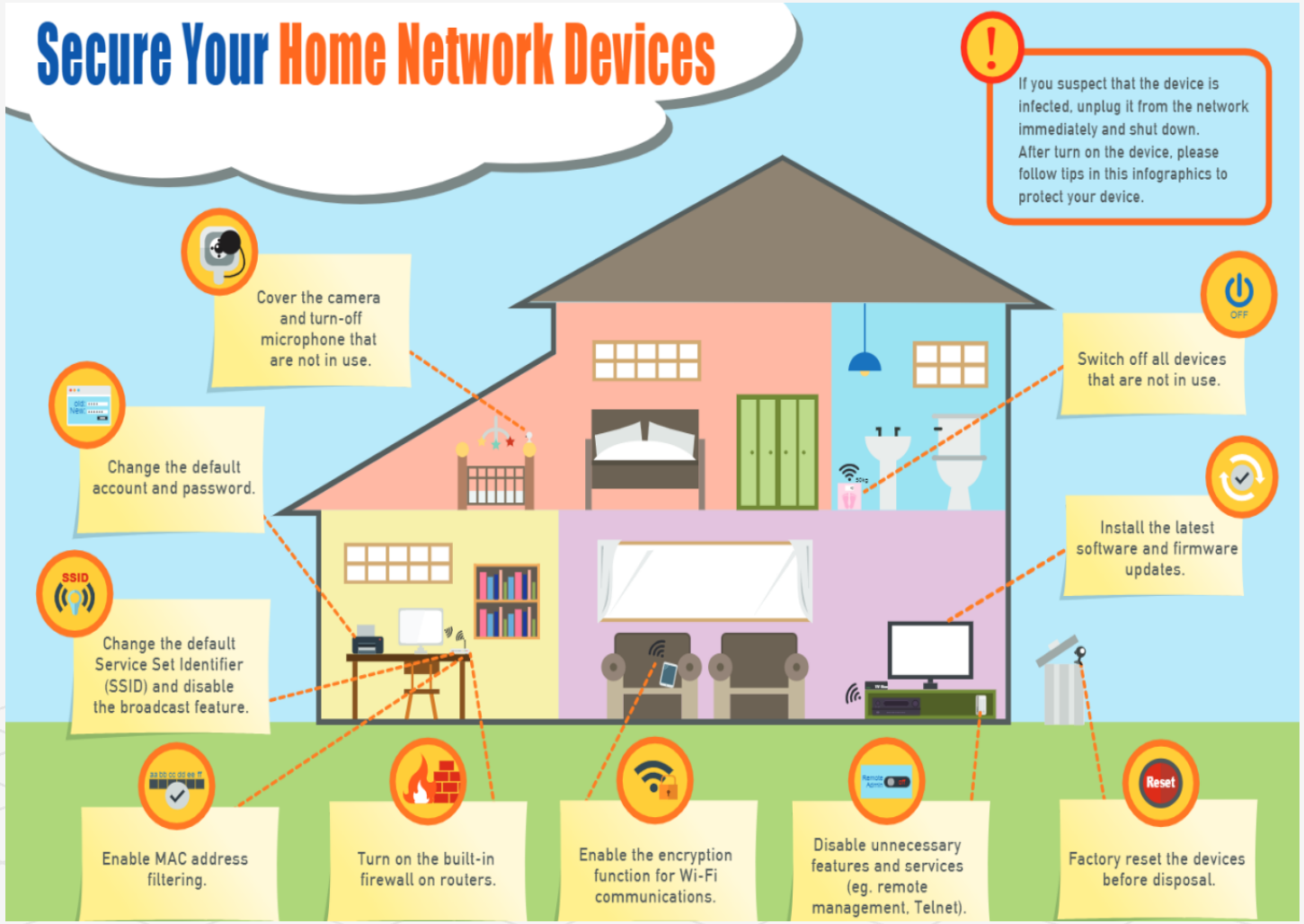
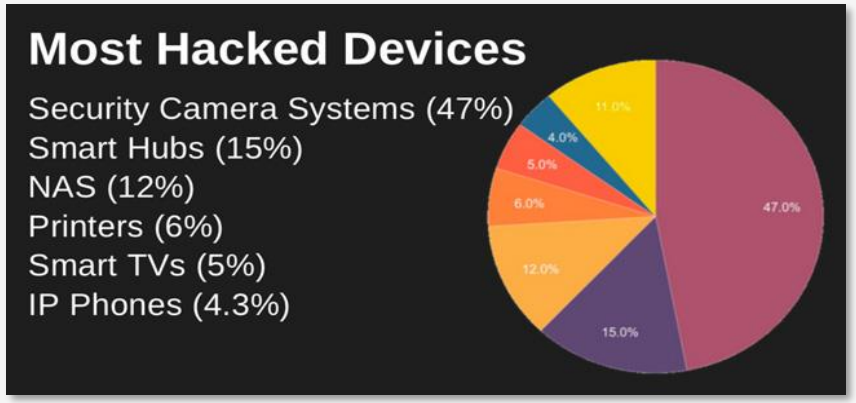


Image courtesy Office of the Government Hong Kong

Statistics: The Internet of Insecure Things



- A study of more than 100 consumer-grade **routers** from seven, mostly large vendors found nearly all tested **routers** are affected by scores of unpatched and often severe security flaws that leave devices and users at risk of cyberattacks. (HelpNetSecurity)

- 1 in 36 mobile devices had high risk apps installed. (Symantec)

- 61% of organizations have experienced an IoT security incident. (CSO Online)

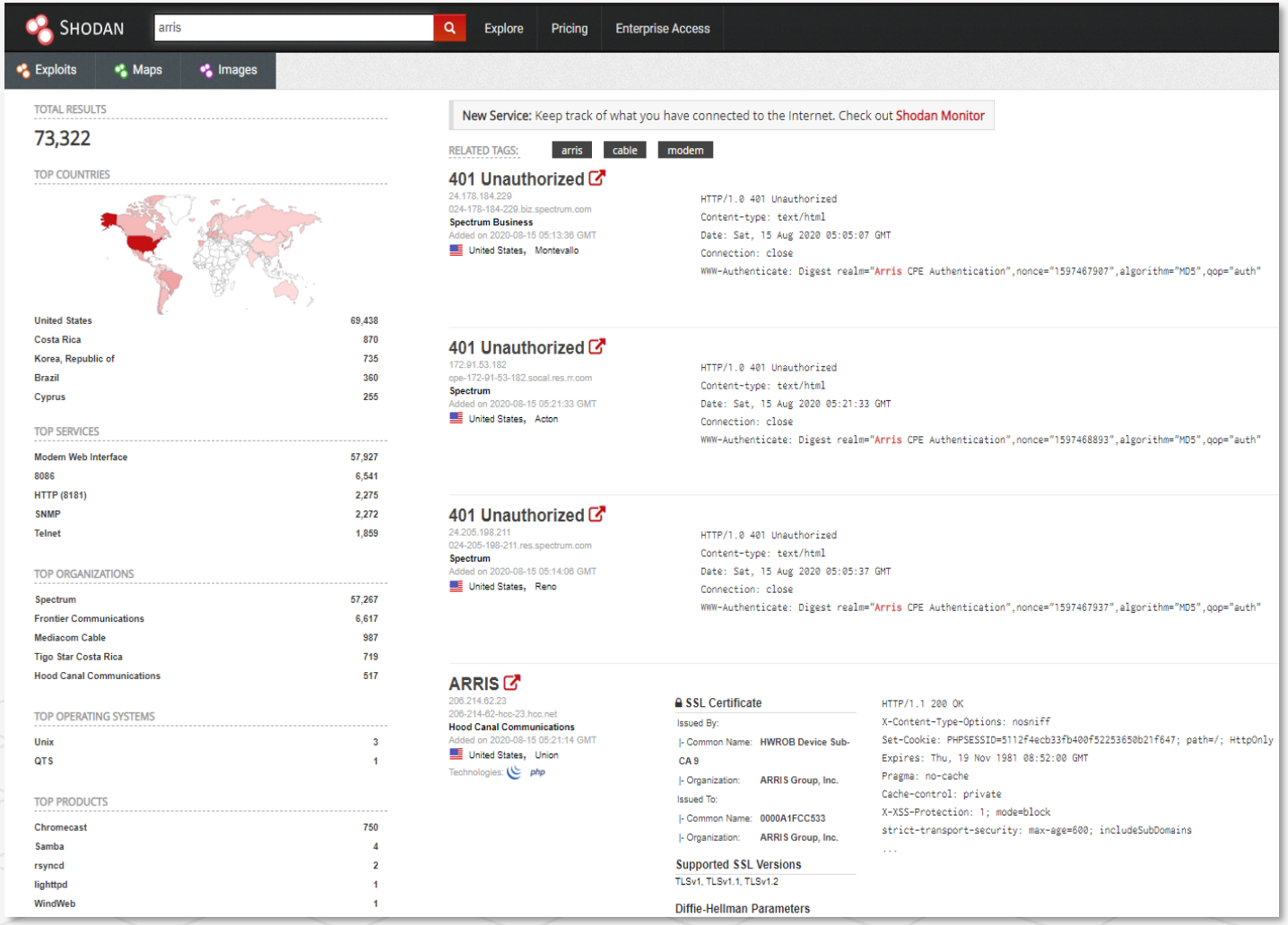
- IoT devices experience an average of 5,200 attacks per month. (Symantec)

- 1 in 13 web requests lead to malware. (Symantec)

Image courtesy HelpNetSecurity.com - June 13, 2019

Hackers: Why Would They Target My Home

It's not about YOU. Scanning tools such as Shodan and Censys are able to quickly scan the whole internet for exposed and vulnerable devices such as routers, webcams and IoT devices.
Typically attackers want to abuse the device's computing power and internet bandwidth to perform their task or crime.
Automated exploitation of these vulnerable devices gives remote control to attackers and the device is added to a "Bot Army". These can amass more than 350,000 bot-infected devices used for DDoS, cryptomining or brute force login attacks from their numerous IPs.

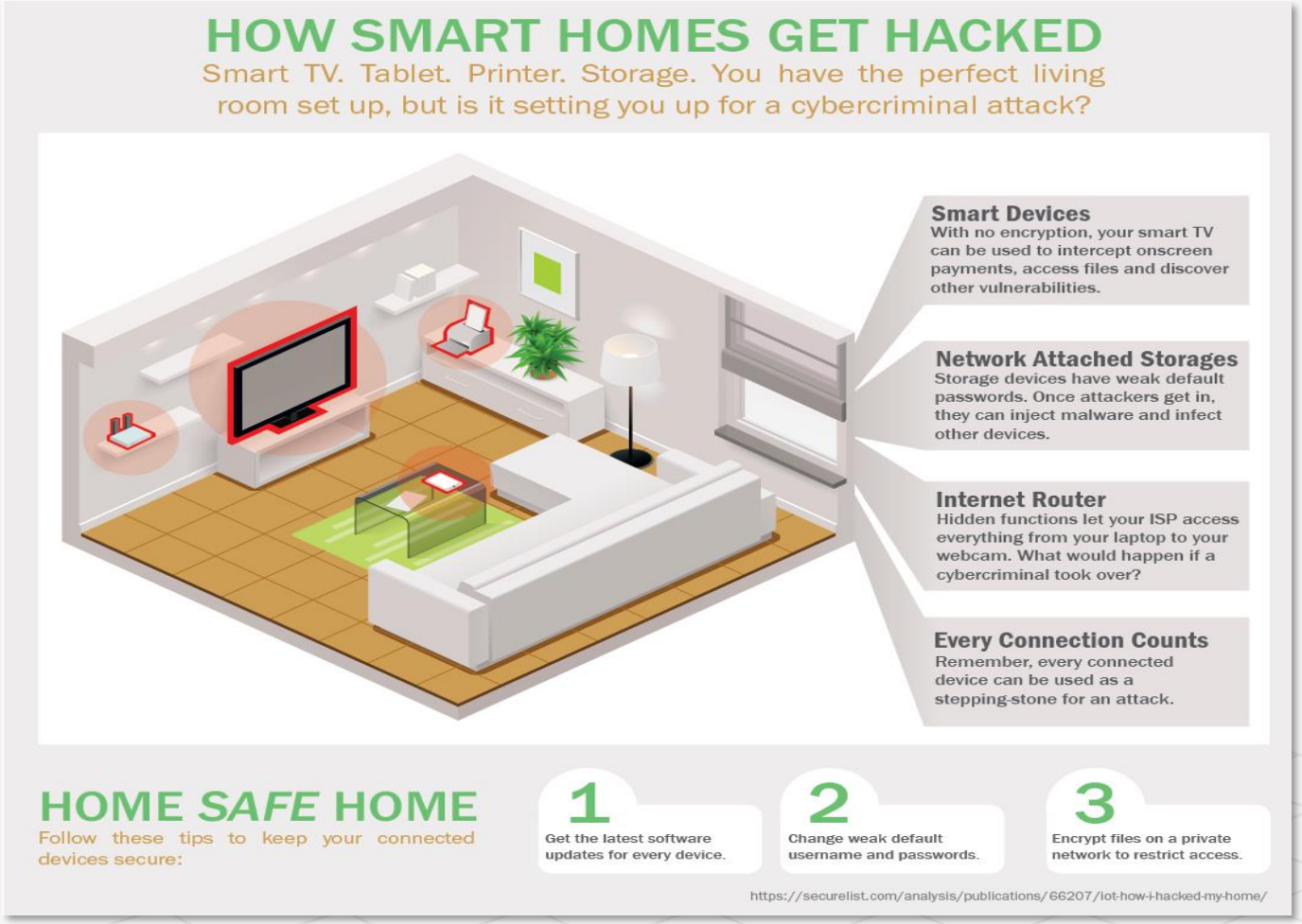


Asset Management 101: Inventory Your Devices

One of the most critical tasks in securing home networks is to inventory all devices that connect to your home network via wi-fi and cable.

The SANS Top 20 Critical Security Controls lists **Hardware** and **Software** Asset Inventory as the #1 and #2 controls in mitigating cyber risk.

Knowing what is connected and what software you have is key to patching and securing your home network.



Prioritizing Risk: Devices & Patching

1. Compile a comprehensive list of your home's internet-connected devices. Your router admin console should show connected devices and their unique identifier or MAC address.

2. Start with your internet provider's on-premise equipment: routers, cable/DSL modems, LTE smart hubs, fiber devices, home alarms, alarm UPS, etc.

3. Do a little research on devices: Search Brand Name/Model of Router + "Vulnerabilities"

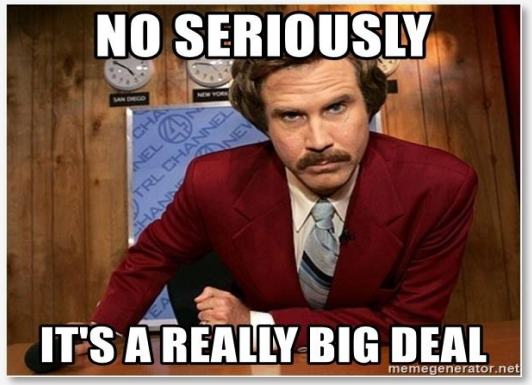
4. Ask your ISP how to patch your router/modem or if you are eligible for an upgrade to a newer model with enhanced security features.

5. Log in to your router/modem's Admin console and disable WEP, WPS, UPnP, and Remote Administration (UPnP is like an open door to hackers). Choose WP2 vs WPA.

6. Turn off unused devices and upgrade end-of-life devices that cannot be patched.

My ISP wouldn't do that…would they?

Three malicious bot armies are competing for your home router and IoT devices: Mirai, Kaiten and Qbot. In December 2019 Trend Micro detected over 249 million brute-force login attempts against residential routers. Attacks have slowed to 193 million in March this year. Many of these brute-force attempts came over telnet, the remote connectivity tool for administering home broadband routers. These devices are highly valued by cyber criminals when coordinated as a "bot army".



Select your Router Manufacturer to find the default password:
https://www.routerpasswords.com/router-password

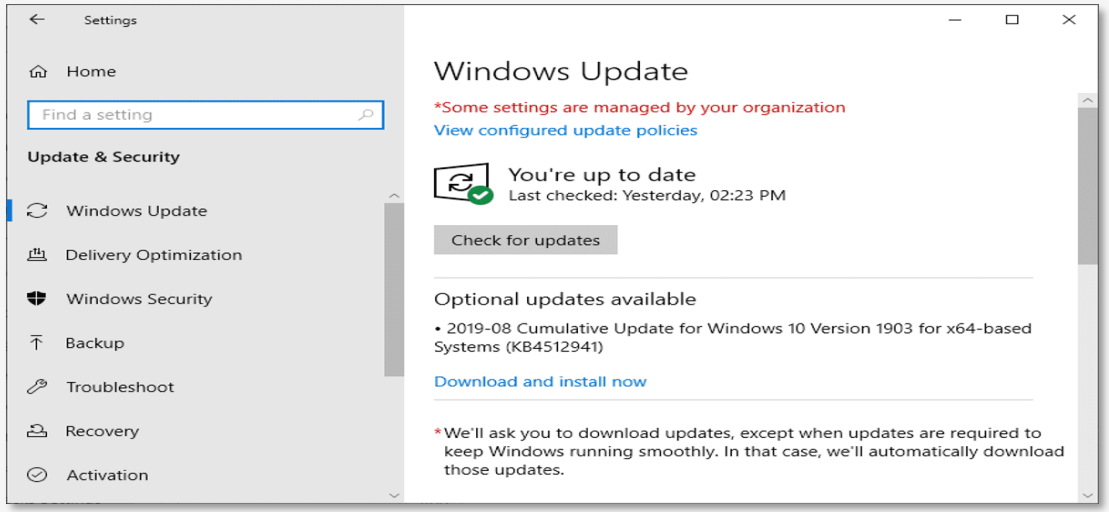
Manufacturer	Model	Protocol	Username	Password
ARRIS	TG1682G		admin	password

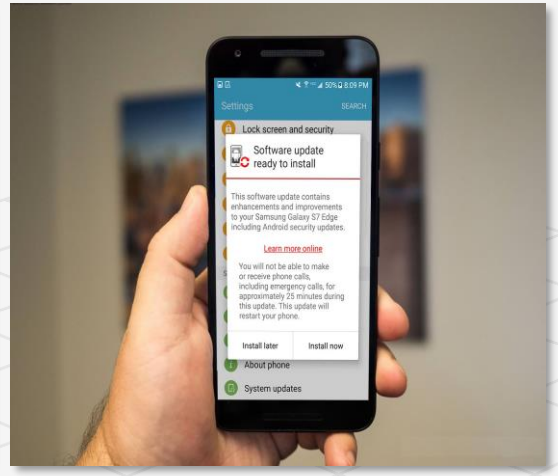
Updates: Software & Firmware

1. **Update your smartphone** when it alerts you that updates are available (that means ASAP). Apple and Google updates secure our devices from new, actively exploited 0-Day attacks.

2. **Update your web browser** (no they don't all auto-update all the time) and limit the number of browsers in use unless you are a web developer and require them all (Firefox, Chrome, Edge, Mozilla, Explorer, etc.).

3. **Update Windows/MacOS/Linux** regularly (including that annoying reboot bit). Deferring or cancelling them is not a secure practice and leaves you vulnerable to malware and device takeover.





BYOD: Why We Can't Have Nice Things

1. Corporate BYOD policies and MDM (Mobile Device Management) are still slow in adoption leaving many employees using personal smartphones vulnerable to attack.

2. Antivirus for laptops, desktops, and mobile devices is a critical control to protect from malware infections.

3. Schedule daily virus scans. Use more than one AV product to ensure overlap.

4. Update your antivirus definitions to detect 0-Day and new malware.

5. Consider using a VPN and restricting Admin rights to laptops and desktops.

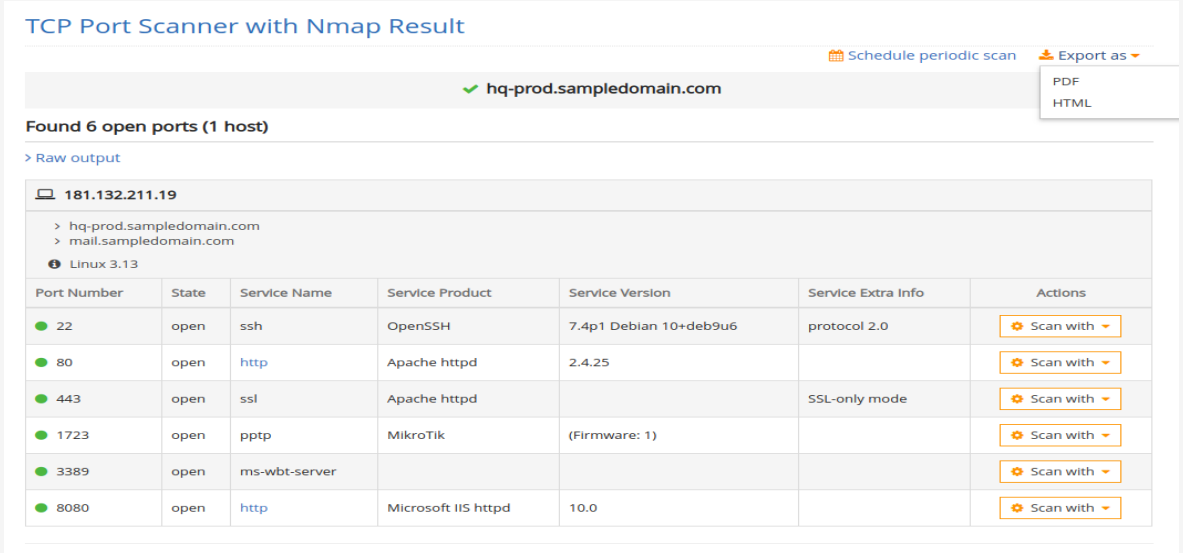
Attack Surface: How to Check Your Exposure

External port scans look for open ports and services like an attacker doing reconnaissance on a target. Ports exposed to the internet (those **4 Billion internet users**) should be the minimum required and reviewed.

Your home internet router's built-in firewall may have settings such as Low/Medium/High. Keep in mind the "High" setting may block social media app functions (ports) like Voice/Video or IoT devices using non-standard ports.

Online Port Scanners can be used to scan your IP address and indicate exposed services and ports: https://www.whatsmyip.org/port-scanner/server/

Port #	Application Layer Protocol	Type	Description
20	FTP	TCP	File Transfer Protocol - data
21	FTP	TCP	File Transfer Protocol - control
22	SSH	TCP/UDP	Secure Shell for secure login
23	Telnet	TCP	Unencrypted login
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP/UDP	Domain Name Server
67/68	DHCP	UDP	Dynamic Host
80	HTTP	TCP	HyperText Transfer Protocol
123	NTP	UDP	Network Time Protocol
161,162	SNMP	TCP/UDP	Simple Network Management Protocol
389	LDAP	TCP/UDP	Lightweight Directory Authentication Protocol
443	HTTPS	TCP/UDP	HTTP with Secure Socket Layer



Questions / References / Resources

1. Your router's security stinks, here's how to fix it
https://www.tomsguide.com/us/home-router-security,news-19245.html

2. Trend Micro Says Botnet Families Fight for Control of Vulnerable Routers
https://www.bankinfosecurity.com/hacker-battle-for-home-routers-a-14706

3. What is UPnP & Why is it Dangerous?
https://www.varonis.com/blog/what-is-upnp/

4. Popular home routers plagued by critical security flaws
https://www.welivesecurity.com/2020/07/09/popular-home-routers-plagued-critical-security-flaws/

5. Most Popular Home Routers Plagued by Known Vulnerabilities
https://www.cpomagazine.com/cyber-security/most-popular-home-routers-plagued-by-known-vulnerabilities-which-vendors-continue-to-ignore/

6. Check Point Research - Business and Home Networks Can Be Hacked from a Lightbulb
https://blog.checkpoint.com/2020/02/05/the-dark-side-of-smart-lighting-check-point-research-shows-how-business-and-home-networks-can-be-hacked-from-a-lightbulb/

7. Don’t be silly – it’s only a lightbulb
https://research.checkpoint.com/2020/dont-be-silly-its-only-a-lightbulb/

8. Surge in remote working reveals concerns around unprotected endpoints
https://www.helpnetsecurity.com/2020/04/17/unprotected-endpoints/