SAM
SEAMLESS NETWORK

2020 IoT security landscape

www.securingsam.com

Our team of researchers developed an overview of IoT security discoveries and recommendations as it relates to home and SMB networks.

This information is based on the most up-to-date research, recent security sources, and data collected from 100M devices and 2M networks.

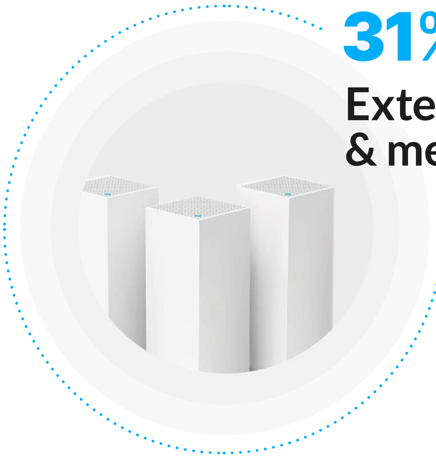
Published vulnerabilities in IoT [i]

We've analyzed all published vulnerabilities during 2020. These vulnerabilities are discovered by researchers and vendors and published on public databases. **More than 200 vulnerabilities** published this year affect IoT devices found in home and SMB networks, and are exploitable from the network.

The most vulnerable device categories include:

12%

VoIP



31%

Extender & mesh

32%

Camera & DVR

IP cameras (and auxiliary equipment such as DVRs)

26%

NAS devices

[i] Based on the National Vulnerabilities Database https://nvd.nist.gov/

Most critical threats

By combining our research with the insights we collected from our fingerprint capabilities, we ranked the most critical threats of 2020 based on the following criteria: **severity of exploit, popularity of device, and potential impact.**

Risk **10**

Western digital my cloud NAS devices

9 vulnerabilities were discovered in 2020 alone, some ranked with the worst risk score by the national vulnerability database. Popular amongst consumers, this device poses a growing threat vector in the IoT space.

Risk **10**

QNAP NAS devices

With at least 15 vulnerabilities in 2020, many are high severity, allowing complete takeover of the device and malwares to spread in the wild. This NAS device poses a major threat to consumers.

Risk **9**

TCL Smart TVs

This extremely popular smart TV is at risk to consumers because of an easy to exploit vulnerability that exposes sensitive information from the device, as well as an ongoing investigation indicating a possible backdoor.

Risk **8**

Orbi Mesh devices

Multiple vulnerabilities were discovered in these Wi-Fi network extender devices. Takeover of any of these devices poses a threat to other devices in the home.

Risk **7**

Grandstream VoIP phones

In the work from home era, business VoIP phones have become more popular. A vulnerability discovered in 2020 allows complete takeover.

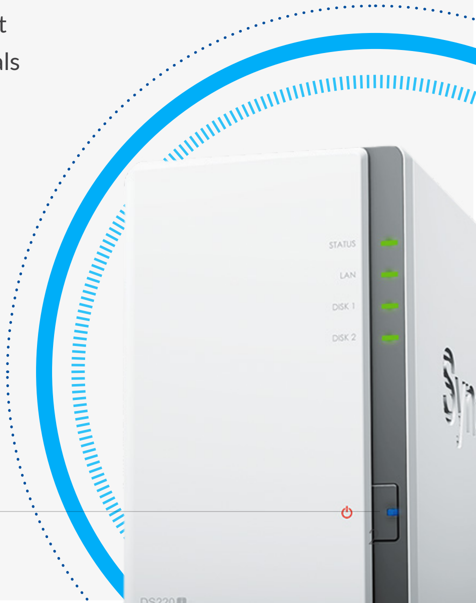
NAS devices – extremely vulnerable

Capturing the attention of security researchers this year, NAS devices have proven extremely vulnerable with more than **30 vulnerabilities** uncovered this year alone. These devices are used by individuals and companies alike for storage of personal data.

Leading vendors for affected devices include QNAP, Western Digital and Zyxel. A dedicated QNAP malware named “QSnatch” has infected more than 62,000 devices across the globe.

30 vulnerabilities discovered in 2020 alone

NAS Devices
These devices are connected to the internet and are used by individuals and companies alike for storage of personal data.



Vulnerabilities that impact millions of IoTs

Security researchers have found vulnerabilities in 5 different TCP/IP stacks – a common component found in every operating system and IoT device. These components are shared by millions of IoT devices by many different vendors.

See the full publications of the researchers:

- RIPPLE20 vulnerability
- AMNESIA:33 vulnerability

IP Cameras are the riskiest smart devices in home networks

Devices in internal networks are most frequently hacked when users expose their device to the internet by opening a port forwarding on the gateway. This opens a large attack surface for hackers to infiltrate the device and the internal network.

We've analyzed port forwarding on more than 1M routers to determine which devices are most exposed. More than 95% of exposed devices are IP cameras.

Since IP cameras are also the most vulnerable device, they are the riskiest IoT devices in small and medium networks.

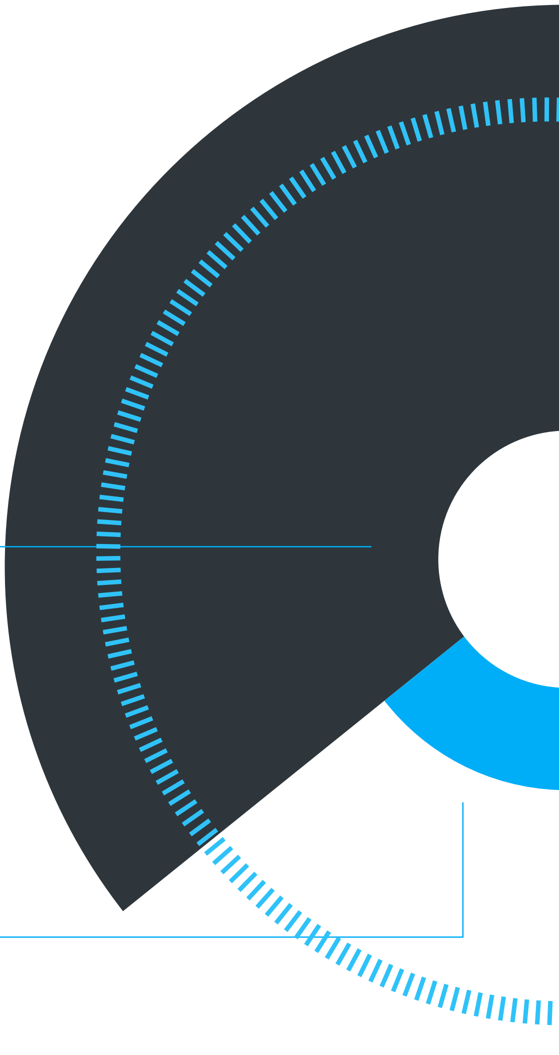
After cameras, NAS devices are most exposed, and also extremely vulnerable.

Port forwarding
An example is when a user attempts to access their IP camera when outside of the home network.

Devices exposed to the internet

95% of exposed devices are IP Cameras

5% Others



Old attacks still circulate

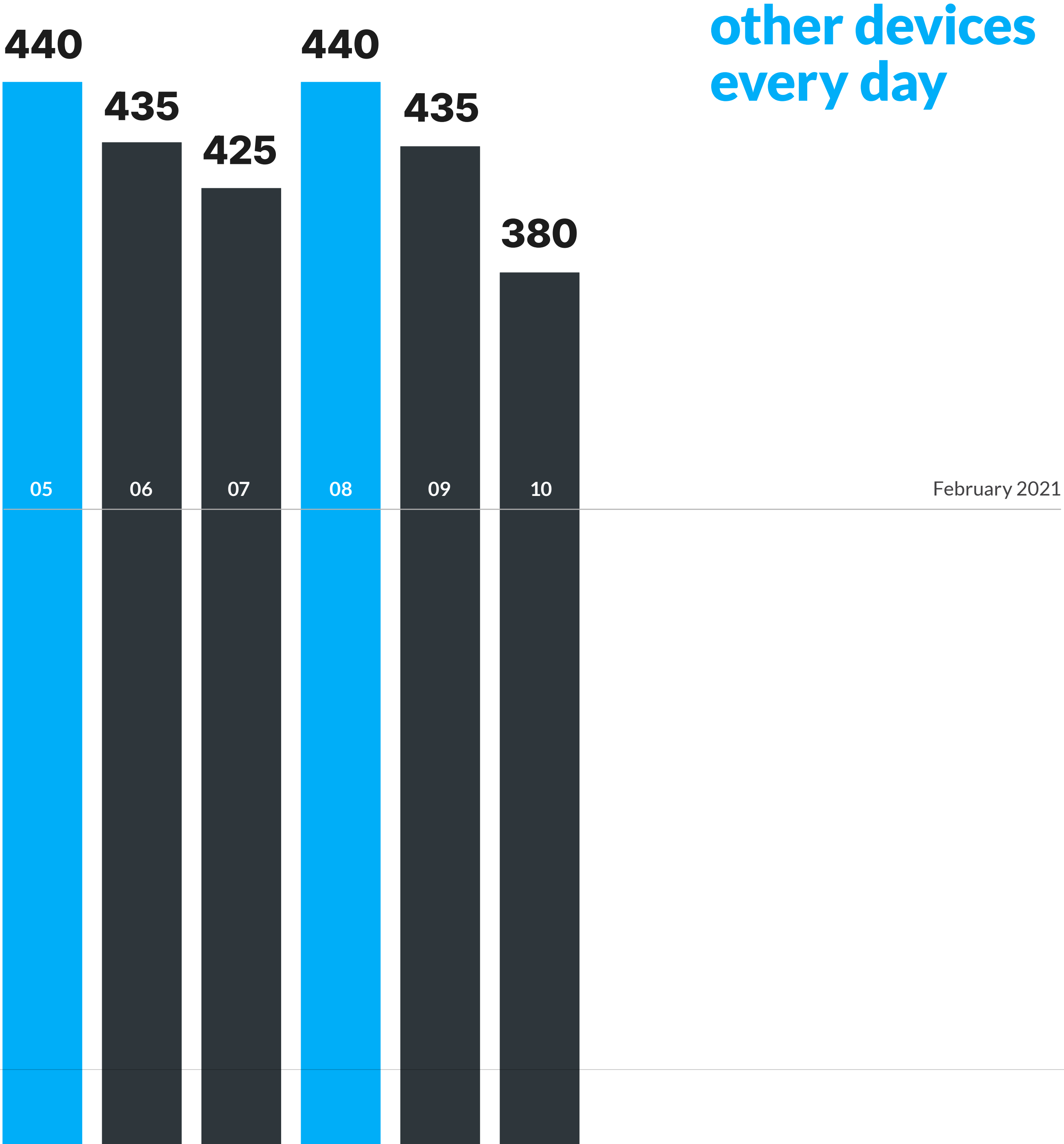
A characteristic of the IoT attack landscape is that old vulnerabilities and attacks are reused for years. In part, this is because users do not necessarily upgrade their devices, and old attacks are still effective.

The Mirai malware

The infamous Mirai malware from 2016 has since evolved to many other variants. One notable variant still circulating, is now called **Mozi**.

A single device infected with Mozi will attempt to infect 400-500 other devices every day

Daily hacking attemps by a Mozi infected device:

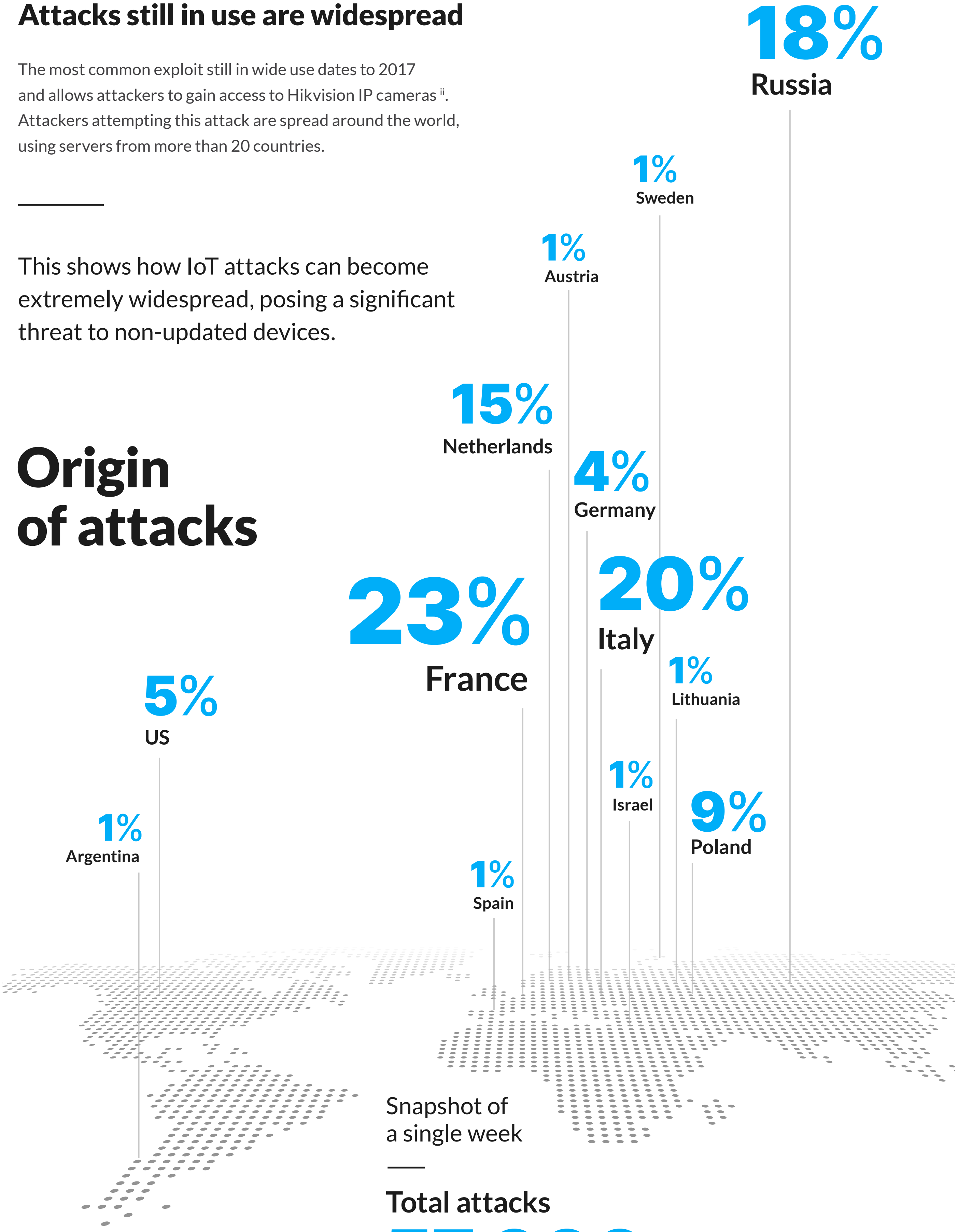


Attacks still in use are widespread

The most common exploit still in wide use dates to 2017 and allows attackers to gain access to Hikvision IP cameras [ii]. Attackers attempting this attack are spread around the world, using servers from more than 20 countries.

This shows how IoT attacks can become extremely widespread, posing a significant threat to non-updated devices.

Origin of attacks



Snapshot of a single week

Total attacks

57,000

[ii] This vulnerability is known as CVE-2017-7921

Recommendations

Considering the above threat landscape,
our recommendations for users are simple yet effective:

Never expose devices to the internet

IP cameras and NAS devices in particular are extremely vulnerable.

Use a VPN instead if you need secure access to your device.

Keep your devices up to date

Most IoT malware exploit known vulnerabilities that can be patched using a firmware update.

Some IoT devices require regular updates, at least once a month.

Secure the IoTs in your network

With a security service that includes virtual patching and monitors device behavior to solve vulnerabilities and block attacks.

SAM protects IoT devices by installing a thin agent on the gateway. It employs virtual patching to automatically secure IoT devices against old and new threats alike, without user intervention.
It constantly monitors device behavior in order to identify emerging threats and protect against them.

Contact us

For more information about SAM Seamless Network, visit our website, securingsam.com or contact us at info@securingsam.com

SAM
SEAMLESS NETWORK

Israel - Headquarters
Totseret Ha'arets 7, Tel Aviv

New York Office
488 Madison Ave, 11th Floor, NY 10022

Berlin Office
5, Schinkelpl, 10117 Berlin

Sources

1. "19 Zero-Day Vulnerabilities Amplified by the Supply Chain." *JSOF*. 2020. www.jsof-tech.com/disclosures/ripple20/

2. "Amnesia: 33." *Forescout*. 2021. www.forescout.com/research-labs/amnesia33/

3. Black Lotus Labs. "New Mozi Malware Family Quietly Amasses IoT Bots." April 13, 2020. blog.lumen.com/new-mozi-malware-family-quietly-amasses-iot-bots/

4. *National Vulnerabilities Database*. nvd.nist.gov/

5. Zorz, Zlijka. "62,000 QNAP NAS devices infected with persistent QSnatch malware." *Help Net Security*. July 28, 2020. www.helpnetsecurity.com/2020/07/28/qnap-nas-malware/