sam
seamless network

2021

IoT Security Landscape

Foreword

IoT devices have been making headlines for many years now, as their usage has grown quickly in many verticals, including industrial, municipal and consumer.

Similarities are often drawn between IoT devices and PCs and smartphones. There are many similarities, but when it comes to IoT operating systems and communication standardization, there is still a large gap. While nearly all computers run either Microsoft Windows or Apple MacOS, both of which are operating systems that receive best-in-class ongoing support and security updates, there is no real equivalent for IoT devices.

For instance, there are hundreds of IoT OEMs and a number of OS options, such as: "non-OS" (aka, "bare metal"), a specific Linux edition, Android (typically early generation) or another system. As a result of this fragmented approach, most IoT devices receive security updates only for a very limited period of time, if at all. SAM's view on IoT security is that it should move to the networking layer.

Nadav Liebermann
VP Innovation and Data,
SAM Seamless Network

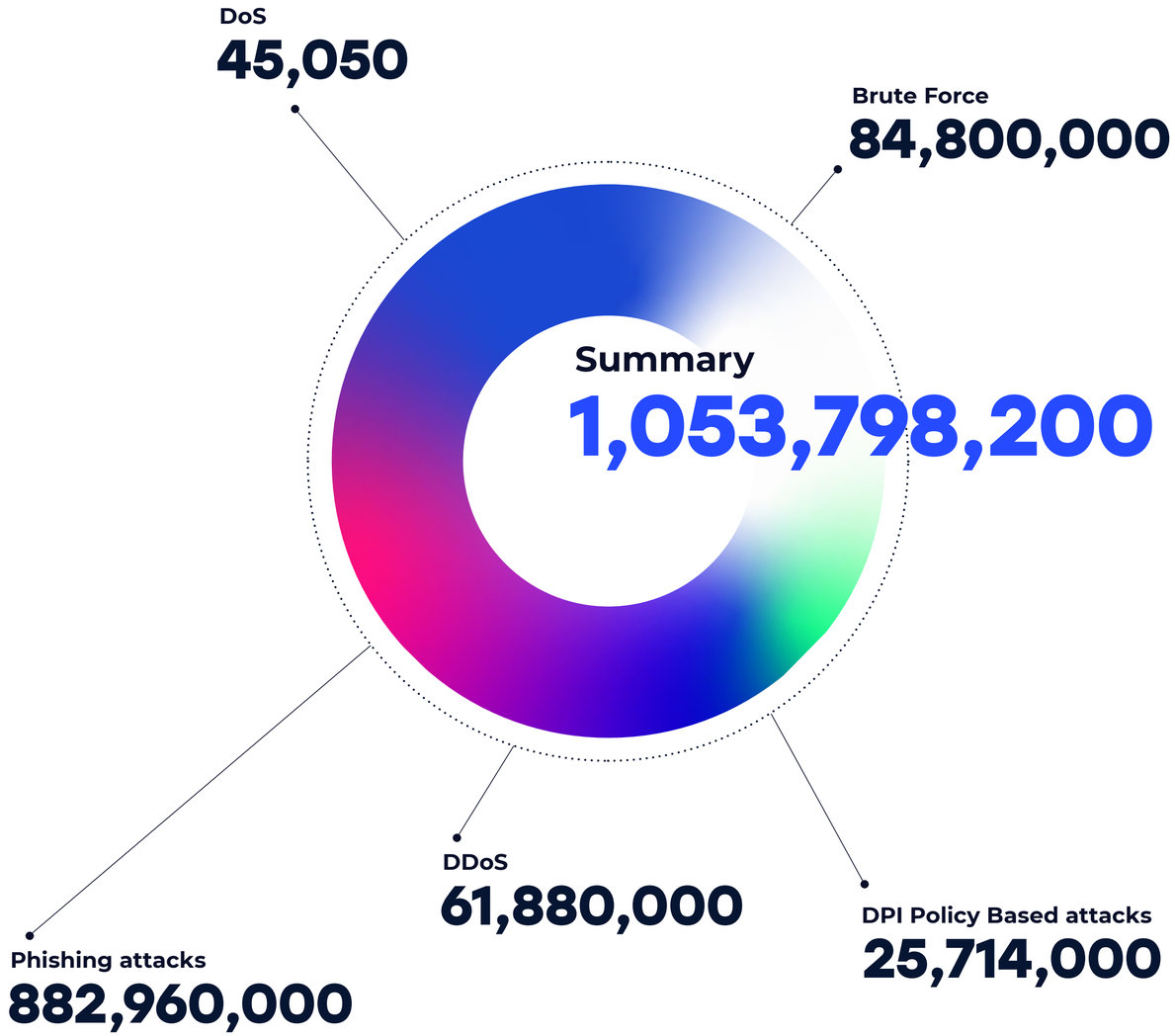
Introduction

1 of 2 networks experience attack or suspicious network traffic behavior

SAM's research team has developed an overview of IoT security developments and discoveries that took place during 2021.

SAM is the leading provider of cloud-native security and intelligence services for unmanaged networks and connected devices, protecting upwards of 370 million connected devices globally. This report's findings are based on in-depth research, security sources, and data collected from **132 million** active IoT devices and **730,000** networks.

We've analyzed DoS, DDoS, brute force attacks, DPI signature-based attacks, phishing attacks and more. More than 1 billion IoT attacks took place during 2021, nearly 900 millions of which were IoT-related phishing attacks.



Our key findings

We combined our research with insights that we collect using our very own **Device Fingerprinting** technology. Here are the threats that stood out to us during 2021.

 |

Mirai and Mozi malware families on the rise

Throughout the course of 2021, malware targeting IoT devices and home routers continued to evolve, with new variants spawning and new exploitation methods constantly added.

Variants of the notorious Mirai botnet have routinely targeted various sets of IoT devices since 2016. Mozi, a 2020 variant of Mirai, specializes in targeting routers and DVRs.

The Mirai and Mozi botnets both added significant new capabilities in 2021. Although some of these threats date back several years, they continue to pose a threat — in fact, they broadened their attack to target additional devices in 2021.

IoT devices used to launch the largest ever DDoS attacks in 2021

A DDoS attack targeted Cloudflare with over 20,000 bots compromised by Mirai with over 330 million requests. These attacks originated from 125 countries around the world, primarily from Indonesia, India, and Brazil.

Another DDoS attack hit Russian internet giant Yandex and security blog KrebsOnSecurity. This attack, known as the Mēris botnet, was conducted by 250,000 compromised devices related to Latvian network equipment vendor MikroTik.

250,000

Compromised Devices

 |

Most Vulnerable IoT Devices in 2021

17% Access points

4% VoIP

3% Cameras

3% Smart home devices

46% Routers

5% NAS

17% Extenders & mesh

Why are routers so vulnerable to attacks (and how can you secure them)?

Routers were attacked most often in 2021 for one simple reason — the vast majority of homes and businesses have at least one! Routers are the nexus of all communication between IoT devices and, as such, are the most vulnerable part of the network. Keeping them secure and updated is something that requires full- time, round-the-clock ‘smart' monitoring.

How can you protect your router from vulnerabilities?

Read our tips on holistically securing a home Wi-Fi network

Here are a few common reasons why routers fall victim to security vulnerabilities:

1. Their passwords and/or credentials are unchanged
2. Their firmware isn’t up to date
3. Network separation (in other words, multiple SSIDs) isn’t being utilized

 |

A snapshot of a single week in 2021

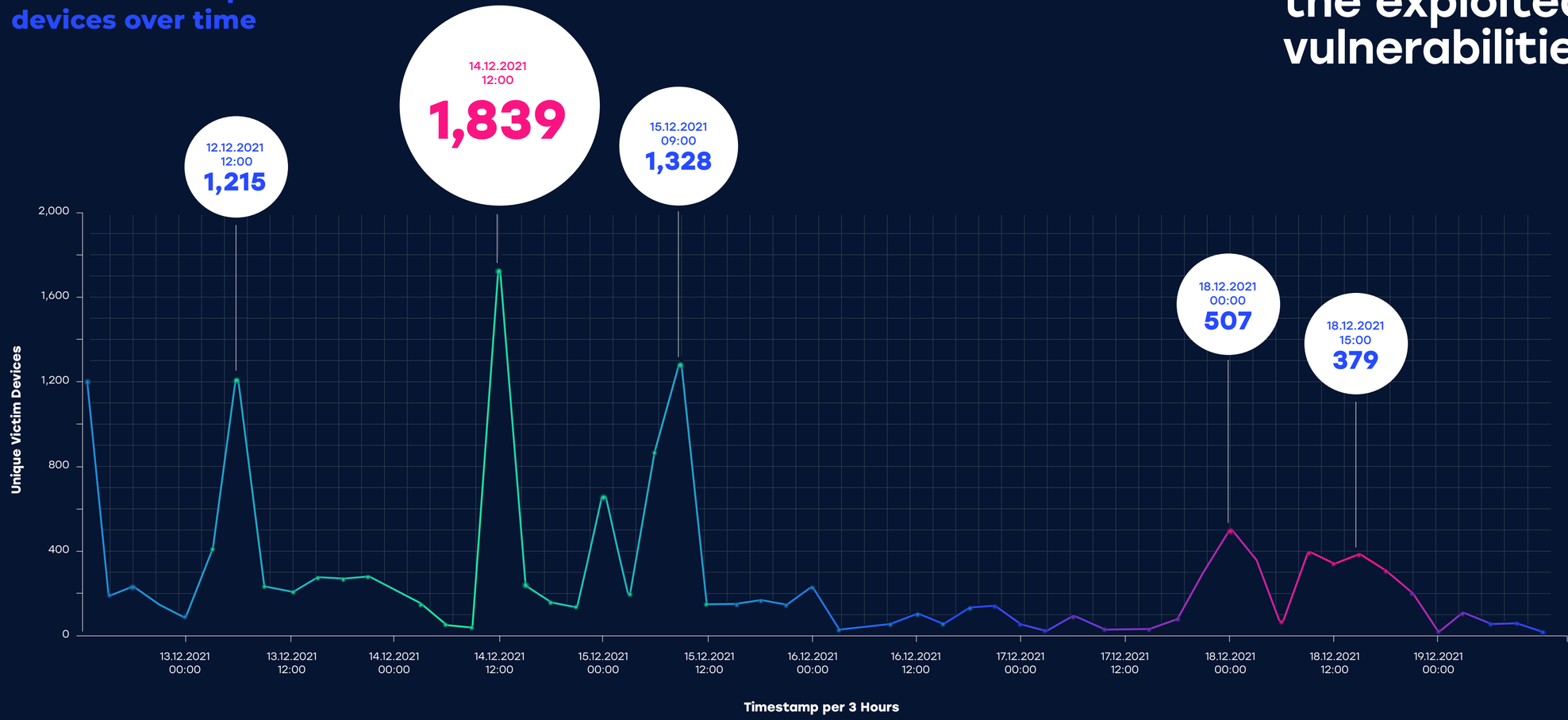
IoT attacks move quickly. Our team has been monitoring the trend of IoT-related vulnerabilities and observing an increased momentum in which they infect and compromise devices.

However, while hackers have crafted attack vectors that spread rapidly, it can take weeks (or sometimes, even months) for firmware vendors to discover, resolve, and patch a vulnerability in their devices. In the meantime, many networks will have already been negatively impacted by the exploited vulnerabilities.

So what does this look like in reality? To put things in perspective, even a week can mean a sharp increase in compromised IoT devices.

When examining the activity of a notable 2021 threat like the Hikvision command injection vulnerability (CVE-2021-36260), we can see just how quickly this threat attacked victim devices. In just one week this vulnerability spread to 3% of our customers' Hikvision cameras and launched almost **10,000 attacks.**

Number of compromised devices over time



Many networks will have already been negatively impacted by the exploited vulnerabilities

A timeline of notable IoT attacks in 2021

FEB

The emergence of Dark, a Mirai variant, targeting multiple routers, firewalls, and IoT devices.

AUG

Dark targets devices with firmware built by Arcadyan only two days after the vulnerabilities are published.

Dark targets devices with SDK by Realtek only two days after the vulnerabilities are published.

Mozi malware evolves to achieve persistence on network gateways manufactured by Netgear, Huawei, and ZTE.

SEP

Meris malware uses compromised MikroTik devices to launch the largest ever DDoS attack on Russian internet giant Yandex.

DEC

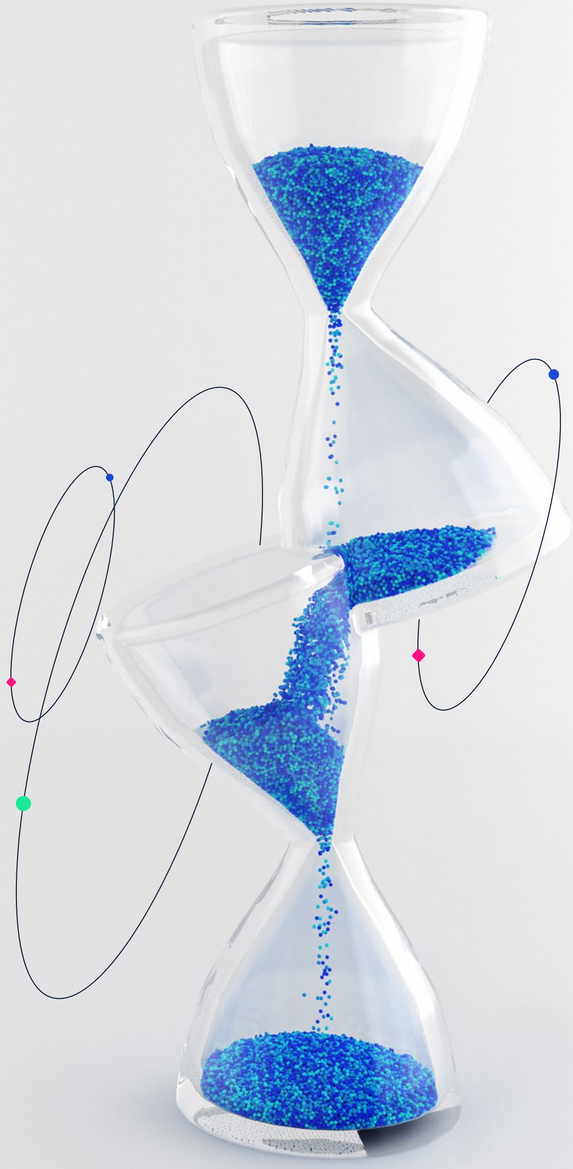
Dark variant targets TP-Link routers.

Moobot, another Mirai variant, starts targeting Hikvision cameras using a vulnerability published in September.

Mirai botnet starts to use the Log4j vulnerability. Researchers witness Log4j used to create Muhstik and Mirai botnets that attacked Linux devices.

How does SAM respond to these threats?

SAM has been studying the behavior of devices for years, building a huge database of devices and communication patterns. Device risk is not static but constantly changing, and we respond by studying the behavior of each device. That way, we can continuously assess the risk that it introduces to a specific network in real-time and take the actions necessary to both prevent and protect against threats.



SAM's most common IoT attacks

Attacks blocked | Compromised devices

[CVE-2017-7921]
Hikvision backdoor
authentication

7,446 | 2,503

[CVE-2021-44228]
Log4j vulnerability
- user agent #2

665 | 610

Multiple CCTV-DVR
Vendors - Remote
Code Execution

1,208 | 370

[CVE-2017-7921]
Hikvision snapshot
disclosure attempt

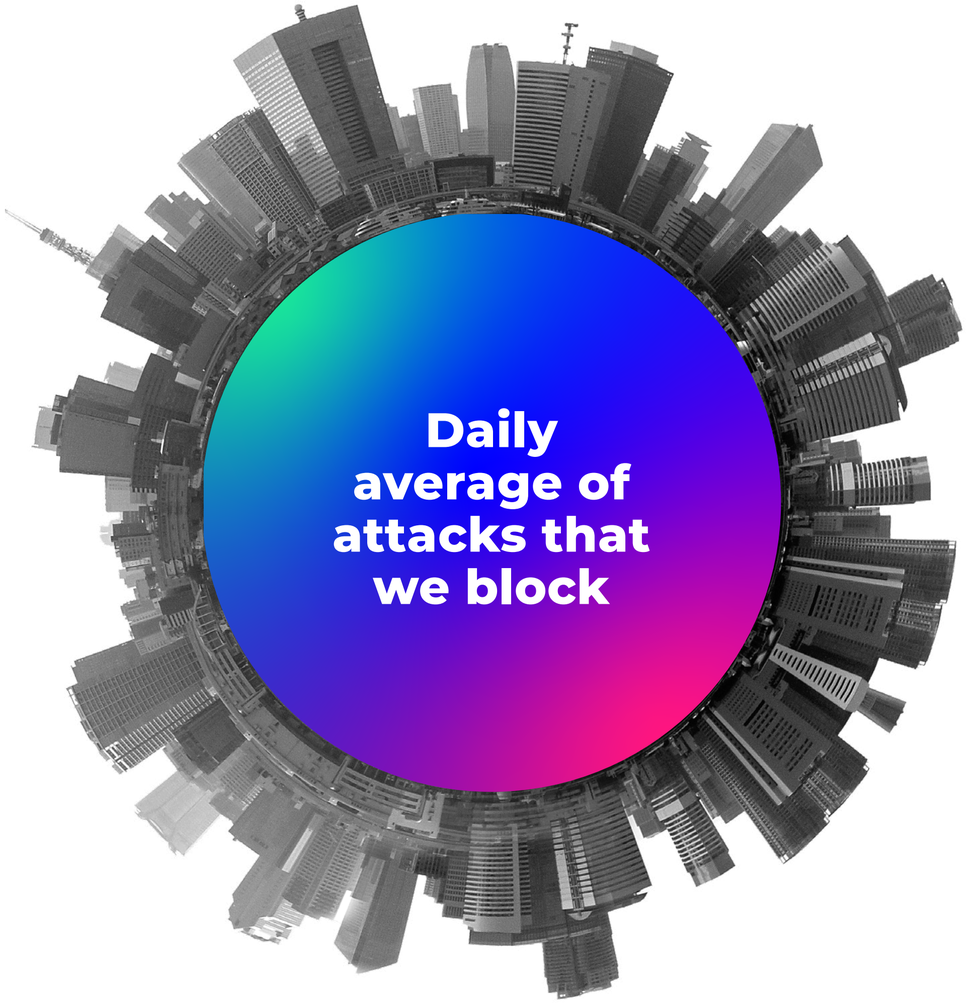
451 | 203

[CVE-2017-18377] Wireless
IP Camera (P2P) WIFICAM
- Unauthenticated Remote
Code Execution

954 | 81

[NO-CVE]
Mozi malware
download attempt

498 | 441



SAM's recommendations for boosting IoT security

Secure home networks to boost privacy

Securing your home Wi-Fi network is paramount when it comes to safeguarding your data. Take a holistic approach to protecting your network by leaning on the expertise of security service providers to make it happen for you. A reliable security provider takes the responsibility of protecting your network, so you don't have to actively work to maintain your security on a regular basis.

Businesses should care about the home networks of their employees

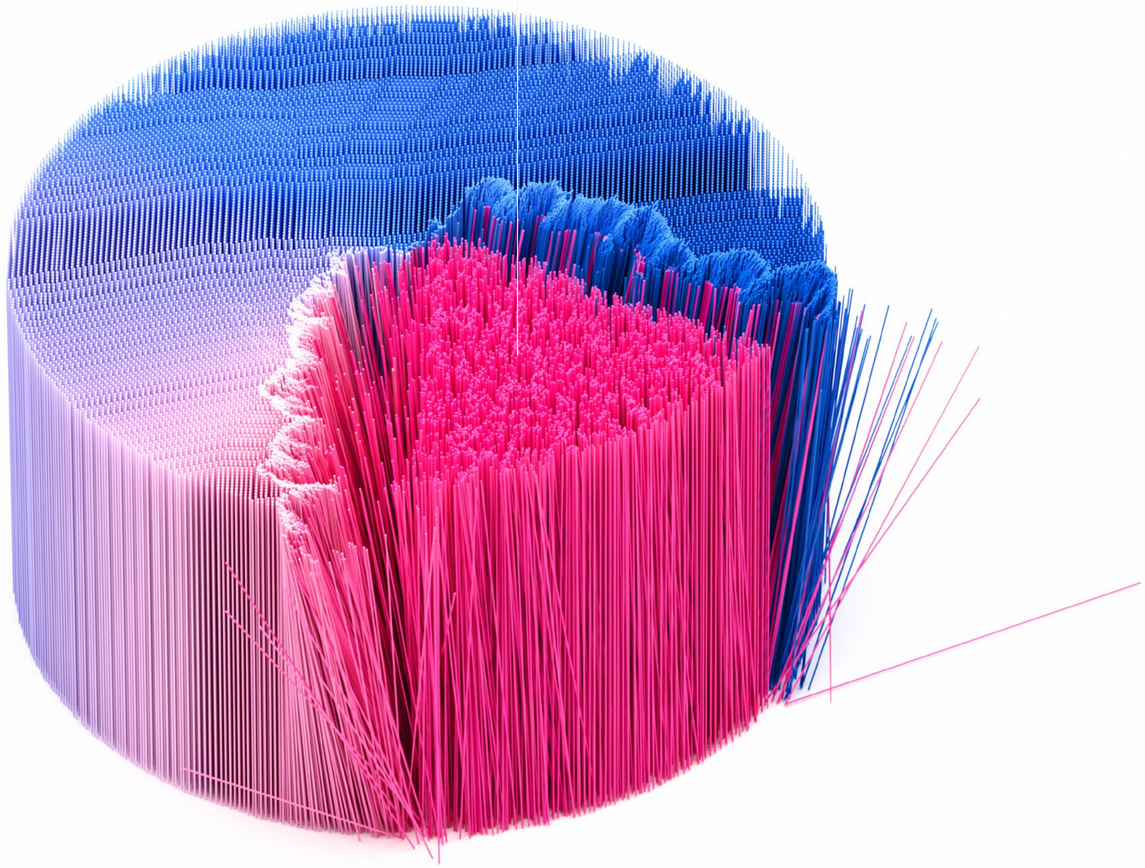
Modern home networks are connected to naturally insecure services, such as IoT devices or legacy routers, that were never designed to confront highly motivated hackers. As the work from home trend continues to grow, it's crucial that today's businesses take **steps to secure the home networks of their employees.**

What’s next for the IoT ecosystem?

We’re living in a world with around 14 billion connected IoT devices, a number expected to reach 31 billion devices by 2025. The IoT market’s growth goes hand in hand with significant innovative technologies, such as, smart homes, 5G, smart cities, cryptocurrencies and decentralized finance, connected cars, and more.

31B

IoT devices expected to reach by 2025



Even though many IoT vendors are concerned about the security of their products, SAM still observes complacency when it comes to applying defense mechanism in practice. Furthermore, our team has analyzed an enormous number of attacks based on older vulnerabilities that initially emerged during the last few years, such as **BotenaGo.** This is to say that there are still compromised devices in the field that have gone without necessary firmware updates for years.

SAM predicts a high correlation between the growth of IoT and the overall related attack surface. As we have explored in this report, malware like Mirai and its variants are still alive and kicking, as are classic attacks such as phishing, DDoS/DoS, command injections, and open port scanners like Shodan. At this point in time, we see zero-day attacks and crypto-hackers as being some of the biggest threats to IoT devices. We predict that the amount of these attacks will continue to grow steadily or, potentially, even exponentially as the market penetration of connected devices continues to expand.

SAM predicts a high correlation between the growth of IoT and the overall related attack surface

 |

About SAM

SAM is the leading provider of cloud-native security and intelligence services for unmanaged networks and connected devices, protecting upwards of 370 million connected devices globally. With its powerful and intuitive AI technology, SAM addresses the unique challenges of our hyperconnected world, in which an explosion of IoT devices exposes potential attack surfaces for companies and consumers alike. SAM's device-agnostic software provides deep network visibility to not only protect against sophisticated cyber-attacks in real-time, but also to prevent the spread of zero-day attacks. SAM's solutions have been designed to study the behavior of a single network of fragmented devices. By using its unique cloud-based device and threat intelligence, SAM identifies every connected device and creates customized protection for all home and SMB users, forming a bulletproof network. SAM's solution is proven to provide telcos with new revenue streams, reduced churn, and minimized support costs through value-added services that strengthen their market positioning and create more value for their customers.

For more information about SAM Seamless Network, contact us ⟶

info@securingsam.com
www.securingsam.com

sam
seamless network

References:

1. “Cloudflare thwarts 17.2M rps DDoS attack — the largest ever reported.” Cloudfare. 2021.
2. “New Mēris botnet breaks DDoS record with 21.8 million RPS attack.” Bleeping Computer. 2021.
3. “KrebsOnSecurity Hit By Huge New IoT Botnet ‘Meris’”. KrebsOnSecurity. 2021.
4. “Many Hikvision Cameras Exposed to Attacks Due to Critical Vulnerability.” SecurityWeek. 2021.
5. “New Mirai Variant Targeting Network Security Devices.” Palo Alto Networks. 2021.
6. “Freshly Disclosed Vulnerability CVE-2021-20090 Exploited in the Wild.” Juniper Networks. 2021.
7. “How to proactively defend against Mozi IoT botnet.” Microsoft. 2021.
8. “Mirai-based Botnet - Moobot Targets Hikvision Vulnerability.” Fortinet. 2021.
9. “Dark Mirai botnet targeting RCE on popular TP-Link router.” Bleeping Computer. 2021.
10. “Log4j RCE activity began on December 1 as botnets start using vulnerability.” ZDNet. 2021.
11. “Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025.” Statista. 2021.
12. “Mirai Botnet Attack IoT Devices via CVE-2020-5902.” Trend Micro. 2020.