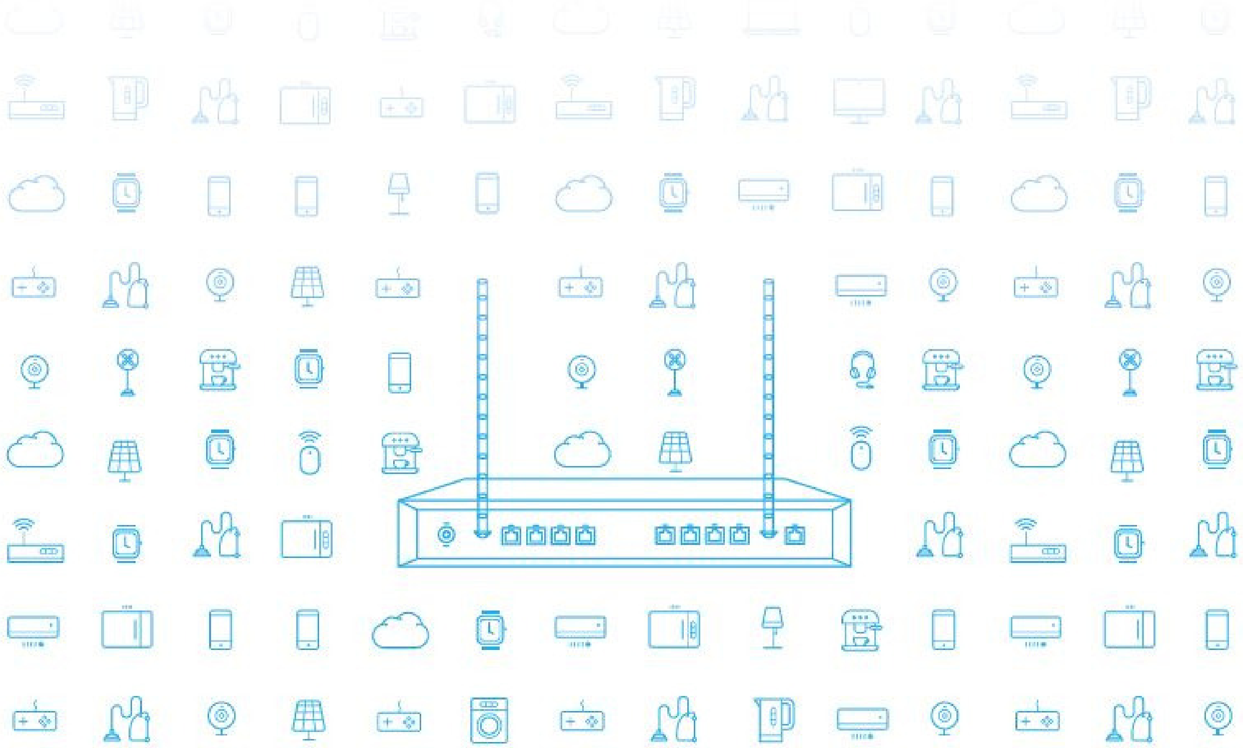
SAM
SEAMLESS NETWORK

An Adaptive Solution That Turns Every Router Into A Smart & Secure Gatekeeper



SAM IN ACTION

Most Common Gateway Attacks

No one wants to believe or admit that they are allowing themselves to be vulnerable to malicious attacks and hackers. Majority of people and companies, if you were to ask them would say that they are protected. However, even the end point devices such as laptops, phones or tablets require manual software updates and password changes in order to be safe from cyber attacks, and research shows few people take these steps due to lack of motivation and understanding on how to take these measures.

The growth of IoT and connected devices in the home and workplace, has only increased these risks and it is easy to be unaware of the security vulnerabilities that come with adding a new and innovative devices such as; smart tv's, camera's, thermostats or video doorbells into your house. Most of these devices have basic integrated software with limited security protocols installed. For example, windows now has 'Windows Defender', a pre-installed but basic anti-virus which the user does not have to install or configure. However, manufactures creating these devices have no experience in cyber security and little understanding of the possible consequences to their users. They also lack the motivation to provide security as demand for their products requires them to be as cheap as possible.

All of these devices are internet or Wi-Fi connected, making the common denominator the home router, which creates an interconnected network of all devices and applications within one's home. Many organizations are developing software's and solutions to help ISP's, as the point of contact for these issues, to take control and responsibility of such security issues. Whether the device is built with ZigBee, Z-Wave, or just Wi-Fi protocols, the data will eventually have to connect to the core network of ISP's - this is why they must begin to take a role in IoT security in order to fully protect themselves and their users.

Tackling the cyber-security problem at the source

Most routers are already built with protective firewalls and most people have some form of security installed on their computers, but if these are left on the default configuration, they still remain easily hacked, something which most consumers are unaware of. The default configuration, in many cases, allows remote access to the router using a known combination of username and password that is the same for all routers of that model. If the attacker can connect to the router using credentials like 'admin' and '1234', he is then able to disable the firewall - ridding of any protection it original provided.

There are many known vulnerabilities in routers and devices, and the reality is that you don't need to be an expert hacker to gain connection to the network. There are reports of existing router vulnerabilities that allowed cybercriminals to identify whether devices have their default credentials or not. Once they have this information, these cyber attackers can gain control or access information from these devices, which exposes the user to an unlimited number of future attacks, especially if not detected for an extended amount of time.

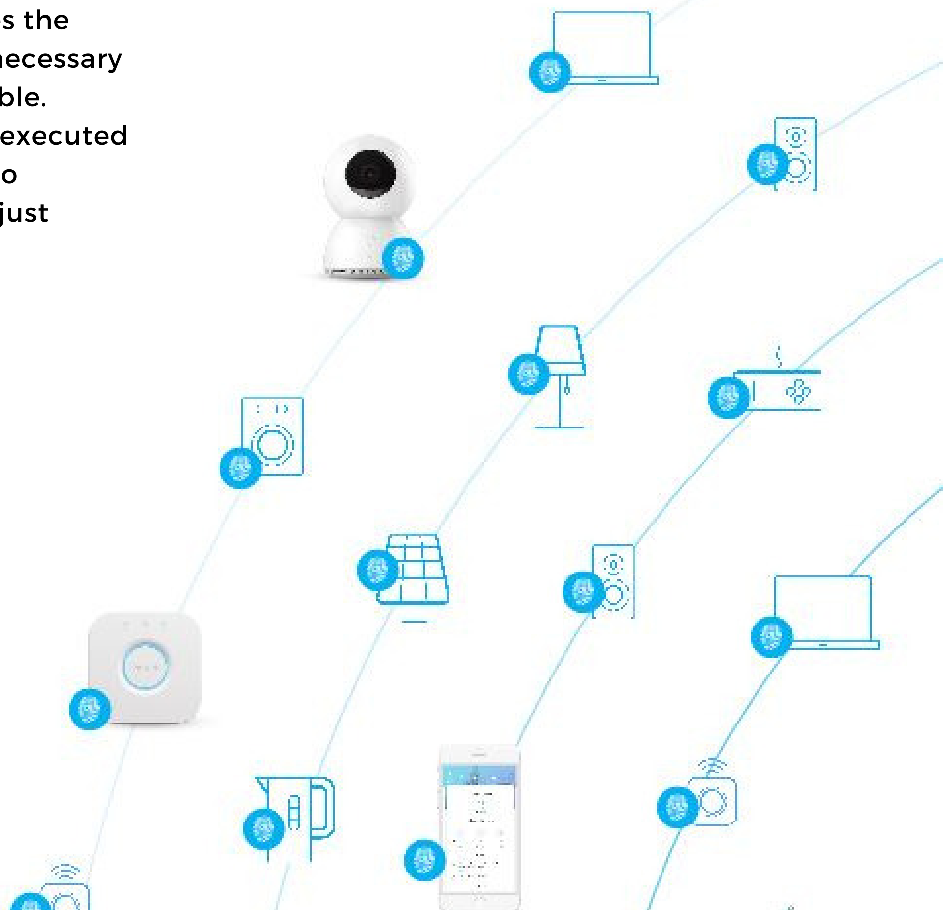
SAM's research shows that the most common attacks on home and SOHO networks are phishing attacks (50%), IoT crypto mining (30%), Ransomware (10%) and Financial trojan (credential theft) (10%). These attacks are spread across the world and don't have a specific country of origin either.

An example of a well-known router hack, is the security vulnerabilities found affecting the ARRIS SURFboard modem (Security Affairs, 2016), which many US internet providers were using and reports stated that more than 135 million devices were at risk. The attackers were taking advantage of many known exploits in the user interface, and the lack of authentication process when accessing the web interface. The attackers were using this hack to reboot routers and force a lengthy 30-minute reset process for consumers, in some casing which even required the support of the ISP. The most common hack through web interfaces is shell command injections. This works by having some input form on the site, the router then takes that input and uses it to format a command to execute on the router. The attacker leverages this to send a malformed input string, resulting in their own command instead of the original command. The attacker then gains full access to the router, which allows them to execute commands and install their malware easily.

The main problem with attacks on router's themselves is that although vulnerabilities are easy to patch as the vendor just needs to update the firmware, this is an expensive, risky and long process. Sometimes the rollout of an update won't happen due to fear of stability regressions and other times the manufacturer doesn't provide the necessary update, leaving the routers vulnerable. Regardless, these updates can't be executed by the end-user alone, the ISP has to distribute the patches themselves, just adding to the complications.

There are also known example for crypto mining such as the SambaCry exploit. This stemmed from the router's other services such as DHCP, UPnP, SMB, SNMP, TR69. Those services are accessible from LAN and in worst case from WAN. The attacker finds an exploit in one of the services and in many cases its a stack overflow, but sometimes it's a logical exploit, like SambaCry. Samba which is a file sharing service for all Linux systems and in this case this is where the attacker used reverse shell to gain remote access and to execute their own commands. This in general gives them the ability to download and run any program from the internet as well as deleting all the data from the victim's computer. They used their access to download one of the most popular open-source cryptocurrency mining tools and in just over a month had successfully mined $5,500 with the number of affected machines remaining unknown.

Many corporate networks, home routers and IoT devices run ancient versions of Samba for file sharing. At the time it was reported that over 110,000 internet accessible devices were running vulnerable versions of Samba, which will plague new routers for years to come, further emphasising the potential of such attacks.



Security Affairs. (2016, April). More than 135 million ARRIS cable modems vulnerable to remote attacks [Blog Post] Retrieved from https://securityaffairs.co/wordpress/46117/hacking/arris-cable-modems-attack.html

SAM’s Solution

At SAM Seamless Network, we protect the home network using the CPE, providing a solution for IoT protection and any network entity.
SAM's solution gathers numerous network parameters to create a sensor, and detects anomalies in the home network, blocking malicious software and viruses.
Through SAM’s technology abnormal behaviors and trends can be identified and we can classify the specific device the virus was coming from.
During one of SAM’s investigations for a European ISP, through SAM’s AI algorithms a vulnerability was discovered on one of their servers and from further investigations we discovered it existed on 1 million routers. With the vast amount of data and DPI logs in the cloud SAM has the insights to discover new vulnerabilities, just like this one which was not known to exist yet. This also gives us the ability to deploy a DPI signature to all affected customers to fully mitigate the vulnerability, quickly and efficiently after the discovery.
Normally to solve such a vulnerability, it would take a long and expensive process through the router’s manufacturer but with SAM’s software the ISP was able to virtually hot patch the vulnerabilities themselves.

In an investigation for another ISP customer, we used our pattern analysis mechanisms which gives scores to each domain based on ML algorithm to uncover vulnerabilities. Here our software found a anomaly, and with our device catalog capabilities, we were able to see all the devices (of customers) who had sent the DNS requests from PC’s running windows. Using this data we created a heatmap of the virus, which showed Russia to be the most infected country, with at least 4700 computers connecting the domain. Further results showed that the malware existed in 178 countries on a total of at least 45K computers. We informed the ISP of this and push notifications were sent to all infected customers with a help page of how to remove the virus. We also blacklisted all the DNS and IP’s related to the malware to further protect our clients.

SAM’s has proven results several ISP’s using different routers and software’s showing our capabilities of blocking and protecting network devices, PC’s, IoT devices etc., using the CPE only and without having any negative impact on the devices or user experience.

Summary

SAM’s research shows how connected devices are on the rise around the world with the average number of devices in homes now at 15 throughout Europe and 17 in the United States.
This IoT and connected future which we are all starting to live was created to make our lives simpler and more convenient, but these new technologies as always come with new security risks. Every day there are new reports of how such devices have been compromised, hacked and used to attack users in different ways.

SAM Seamless Network reacts immediately to any new vulnerabilities in real-time, protecting all networks and devices. SAM’s cybersecurity software protects local area networks and all connected devices directly at the source of entry for the ISPs and telcos via the router. The software is installed on top of any gateway (legacy and pre-market), without necessitating additional manpower, has an ultra-light footprint, and does not require any extra hardware or additions to be installed on the connected devices. SAM’s solution can be optimized for any network by customizing security policies according to the connected devices and their behavioral signature, isolating suspicious entities and using advanced AI algorithms in order to detect anomalies. In addition to cybersecurity abilities, SAM helps telcos and cable operators enrich their value proposition for their customers by providing network visibility, management abilities, and parental control. Sam is partnering with telcos and ISP’s not only for security but also for VAS customer advantages.

SAM
SEAMLESS NETWORK

Book your demo at SAM today
www.securingsam.com