Life Is On | Schneider Electric

Cybersecurity: Securing Home IoT Devices and Networks

Daniel Paillet, CISSP, CCSK, CEH

Executive summary

Internet connectivity is exploding with innovation, enabling homeowners to implement all kinds of home technologies for convenience, lifestyle enhancements, and to be more “green.” Internet of Things (IoT) innovation provides the user with live, up-to-date information on energy usage, including command and control of electrical devices and functions for the home. When deploying such systems and devices, one must be mindful of what security measures should be implemented to mitigate potential cybersecurity attacks on home IoT systems, devices, and home networks.

Introduction

IoT technology provides the ability to access instant information to make decisions on energy usage, door-entry systems, and command and control of lights, smart appliances and electrical outlets remotely from mobile applications. With these points of entry from the internet into home IoT systems, the average homeowner is not only faced with securing external access to these devices but also how these internal devices communicate outwardly to the internet.

Open source firewall vs home routers

Today many ISPs (Internet Service Providers) provide the homeowner with a router that may also include wireless capability. The consumer can also go online or to a local retailer and purchase any number of wireless routers to provide internet connectivity in their home. The internet is less than a friendly place where rogue entities and malevolent characters hunt and search for low hanging fruit to compromise and attack.

There have been several articles showing exploited vulnerabilities on Belkin, Linksys, MikroTik, Netgear, and other home routers. One example occurred where the FBI issued the following:

"The FBI warned on Friday that Russian computer hackers had compromised hundreds of thousands of home and office routers and could collect user information or shut down network traffic."

"The FBI warned on Friday that Russian computer hackers had compromised hundreds of thousands of home and office routers and could collect user information or shut down network traffic."

In Germany, 900,000 Deutsche Telekom customers were knocked offline by an attempt to hijack broadband routers into a botnet.[1] An article found on welivesecurity.com states: Malicious hackers are commandeering vulnerable Zyxel and Speedport routers and commandeering them into a botnet, which they can command to launch huge denial-of-service attacks against websites. The vulnerability exploits the TR-069 and TR-064 protocols, which are used by ISPs to manage hundreds of thousands of internet devices remotely. In this case, an attack was able to fool the vulnerable routers into downloading and executing malicious code with the intention of crashing or exploiting them. Compromised routers could be commanded to change their DNS settings, steal Wi-Fi credentials or bombard websites with unwanted traffic.[2]

Recently, a buffer overflow vulnerability was found on TP-Link routers that can allow an attacker from a remote location the ability to take control.[3] A sample of the details concerning the attack is as follows:

"Looking at the software security of the device, it appears that most of the effort to apply controls was put into the web-based interface that users can access to configure the router. However, controls that were placed on the owner's interface cannot protect the actual router and could allow an attacker to take advantage of that fact."

Home routers do offer ease and convenience to bring internet connectivity to the home; however, the above examples show there are vulnerabilities that can be introduced into the home. Keep in mind that these issues can be mitigated by applying updates provided by manufacturers to secure the home router.

---

[1] https://www.welivesecurity.com/2016/11/29/900000-germans-knocked-offline-critical-router-flaw-exploited/

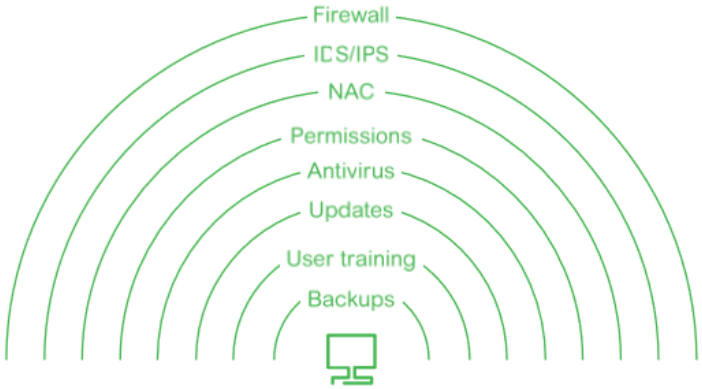
[2] https://www.welivesecurity.com/2016/11/29/900000-germans-knocked-offline-critical-router-flaw-exploited/

[3] https://securityintelligence.com/buffer-overflow-vulnerability-in-tp-link-routers-can-allow-remote-attackers-to-take-control/

Open source firewalls

Open source firewalls can offer the user a component to help support a defense in depth strategy for the home network. Typically, these firewalls are software-based with the user needing to provide the hardware based on the vendor's software specifications. The configurations of these firewalls will require more effort and research to configure and operate than a consumer router. Defense in Depth is an approach to cybersecurity in which a series of defensive mechanisms are layered to protect valuable data and information. If one mechanism fails, another mechanism steps up immediately to thwart an attack. Figure 1 below provides a visual example of defense in depth.

Figure 1



"Looking at the software security of the device, it appears that most of the effort to apply controls was put into the web-based interface that users can access to configure the router. However, controls that were placed on the owner's interface cannot protect the actual router and could allow an attacker to take advantage of that fact."

The homeowner should not rely on NAT[4] (Network Address Translation) to protect a home network but should leverage other capabilities that open source firewalls can offer, such as anti-virus, intrusion detection prevention systems, URL filtering, proxies, geographic Internet Protocol (IP) blocking, and granularity of firewall rules for inbound/outbound traffic for the home network. As far as which open source firewall to choose, the debate between Linux-based vs. FreeBSD UNIX continues to rage with "true believers" on both sides of the camp. Both have advantages and disadvantages, with the homeowner needing to make the decision based on the comfort level and understanding of security and the technical expertise needed to configure such systems. Certain enhancements to secure DNS (Domain Name Services) can also be secured using open source firewalls.

Domain Name Services

DNS is the phonebook of the internet. DNS eliminates the need to memorize IP addresses to find internet sites such as 185.201.54.50 in IPv4, or more complex IPv6 addresses such as 2400:cb00:2048:1:c629:d7a2. To explain the details of how DNS works is out of scope for this discussion; however, there are plenty of internet links available such as the following: https://www.cloudflare.com/learning/dns/what-is-dns/ that explain the technical details. For the purposes of this discussion keep in mind that DNS converts domain names to IP addresses. As DNS is natively insecure, these conversions could be intercepted and maliciously modified, sending your traffic to somewhere other than intended. In the next section, we will look at placing some protections in place to guard against that.

[4] https://computer.howstuffworks.com/nat.htm

In 2007, NLnet Labs[5] released Unbound. Unbound is a validating, recursive, and caching DNS resolver. This software is freely distributed and runs on FreeBSD, NetBSD, Linux, as well as Microsoft Windows. What Unbound DNS provides is the ability to send DNS over TLS. Having DNS over TLS provides the homeowner with the ability to mitigate against MiTM (Man-in-the-Middle) attacks, DNS poisoning, and ISP DNS highjacking. While it is impractical for a user to secure all DNS traffic (due to involving multiple servers interconnected across the internet), the most vulnerable link is the one between the client machine and the next-hop DNS server.

"DNS hijacking or DNS redirection is the practice of subverting the resolution of Domain Name System (DNS) queries. This can be achieved by a malware that overrides a computer's TCP/IP configuration to point at a rogue DNS server under the control of an attacker, or through modifying the behavior of a trusted DNS server so that it does not comply with internet standards.

These modifications may be made for malicious purposes, such as phishing, or for self-serving purposes by Internet Service Providers (ISPs) and public/router-based online DNS service providers to direct users' web traffic to the ISP's own webservers where advertisements can be served, statistics collected, or other purposes of the ISP; and by DNS service providers to block access to selected domains as a form of censorship."[6]

". . . DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer)."[7]

Recently attackers leveraged the Google Cloud Platform to go after unpatched consumer routers.[8] If you do own a consumer router, it is extremely important that you apply updates as they arrive from the manufacturer of your router.

DNS over TLS

In 2019 DHS (Department of Homeland Security) issued a security alert about DNS highjacking attacks. Implementing DNS over TLS adds a level of robustness to mitigate attacks by using secured public DNS servers. Routers that are capable of running OpenWRT[9] versus a low-end consumer home router, can also provide the implementation of Unbound DNS services, which are designed to protect from unintended redirects. Proper implementation of Unbound DNS can provide the resolution of IP addresses with cryptographic signatures to validate the DNS response from the valid and authentic server.[10]

[5] https://nlnetlabs.nl/projects/unbound/about/

[6] https://en.wikipedia.org/wiki/DNS_hijacking

[7] https://en.wikipedia.org/wiki/DNS_spoofing

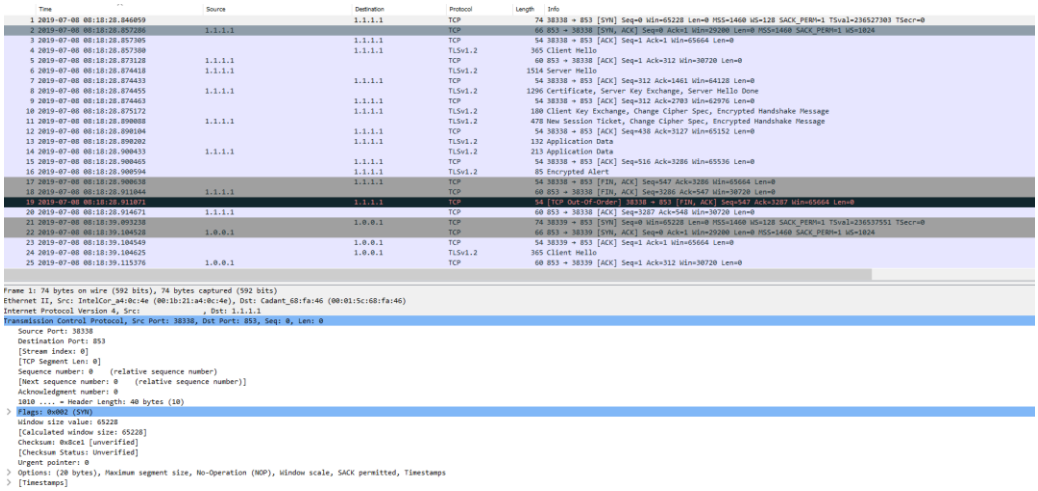
[8] https://arstechnica-com.cdn.ampproject.org/v/s/arstechnica.com/information-technology/2019/04/ongoing-dns-hijackings-target-unpatched-consumer-routers/?amp=1&amp_js_v=0.1#referrer=https%3A%2F%2Fwww.google.com&amp_tf=From%20%251%24s&ampshare=https%3A%2F%2Farstechnica.com%2Finformation-technology%2F2019%2F04%2Fongoing-dns-hijackings-target-unpatched-consumer-routers%2F

[9] Routers running Open WRT can also implement DNS over TLS

[10] https://www.namecheap.com/support/knowledgebase/article.aspx/9717/2232/what-is-dnssec

From an opensource firewall implementing DNS over TLS, we can see a Wireshark example of DNS over TLS in figure 2 below.

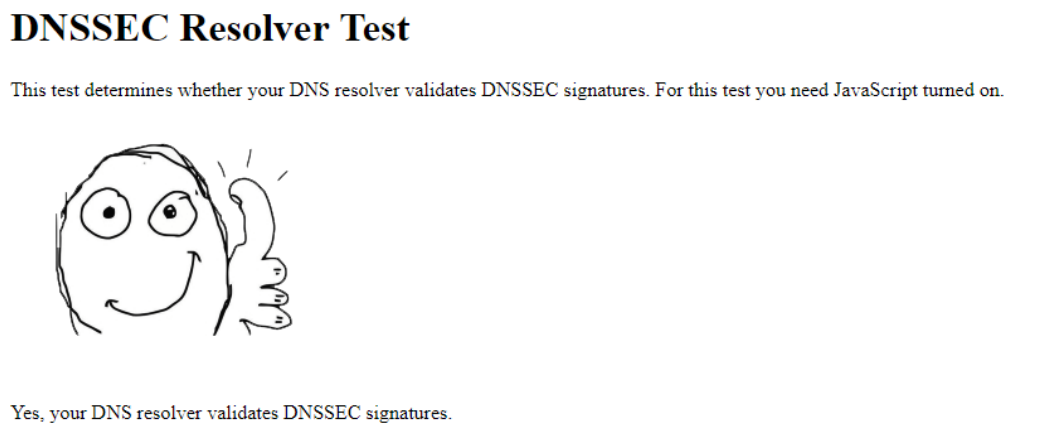
Figure 2



The above example shows the open source firewall resolving DNS over TLS to Quad9[11] servers providing DNS over TLS. Cloudflare[12] provides public servers for DNS over TLS as well. The ability to secure DNS over TLS provides both the home network and IoT devices a greater level of security to send information across the internet via the implementation of Unbound DNS.

To validate the correct implementation of DNSSEC, you will need to temporarily enable JavaScript on your browser. From a computer or tablet inside your home network, use the following link to test your DNS configurations to validate DNS over TLS: https://dnssec.vs.uni-due.de/. Select 'start test' and if successful, you should see the following results as seen in figure 3.

Figure 3



As part of a free service to the user, Quad9 provides the blocking of known malicious domains to prevent your systems and IoT devices from connecting to malware or phishing sites.[13] As for data privacy, Quad9 states the following:

[11] https://www.quad9.net/

[12] https://www.cloudflare.com/dns/dnssec/how-dnssec-works/

[13] https://www.quad9.net/about/

"Privacy: No personally-identifiable information is collected by the system. IP addresses of end users are not stored to disk or distributed outside of the equipment answering the query in the local data center. Quad9 is a not-for-profit organization dedicated only to the operation of DNS services. There are no other secondary revenue streams for personally-identifiable data, and the core charter of the organization is to provide secure, fast, private DNS."[14]

Open source firewalls can also provide the ability to allow inbound VPN (Virtual Private Network)[15] connections into a home network. Some of these VPN connections can be configured over HTTPS/443 into the firewall to allow secure communications to remotely manage IoT devices and home network devices running inside the home.

Securing IoT devices

Homeowners installing IoT devices and systems are subject to hackers coming after those devices and their home network. Examples of such incidences include the following:

- **Nest Camera Hack:** The outreach comes after claims that a US family found out that their Nest security system had been remotely accessed, and the speaker used it to taunt the home's occupants with racist obscenities.[16]
- **Thermostat Hacks**: The HVAC is now facing challenges with hackers attacking Wi-Fi based thermostats.[17]
- **Alexa/Echo Hacks**: Researchers and security experts have found ways to hack into and control these speakers' voice assistants with methods including undetectable audio commands, eavesdropping software and targeting devices connected on a network.[18]
- **Home Car charging systems:** Remotely controlled EV home chargers.

Properly configured Virtual Local Area Networks (VLANs)[19] and subnets can be used to segregate operations and functions of home IoT devices and systems. While this does take a certain level of networking knowledge, if properly done, it can help segregate and isolate household functions from streaming TVs to home computers, lighting systems, and an Electrical Vehicle charging station, as examples. Figure 4 below is an example of a home network showing VLANs and subnets segregating a home network and various IoT systems.

[14] Ibid.

[15] https://www.whatismyip.com/what-is-a-vpn/

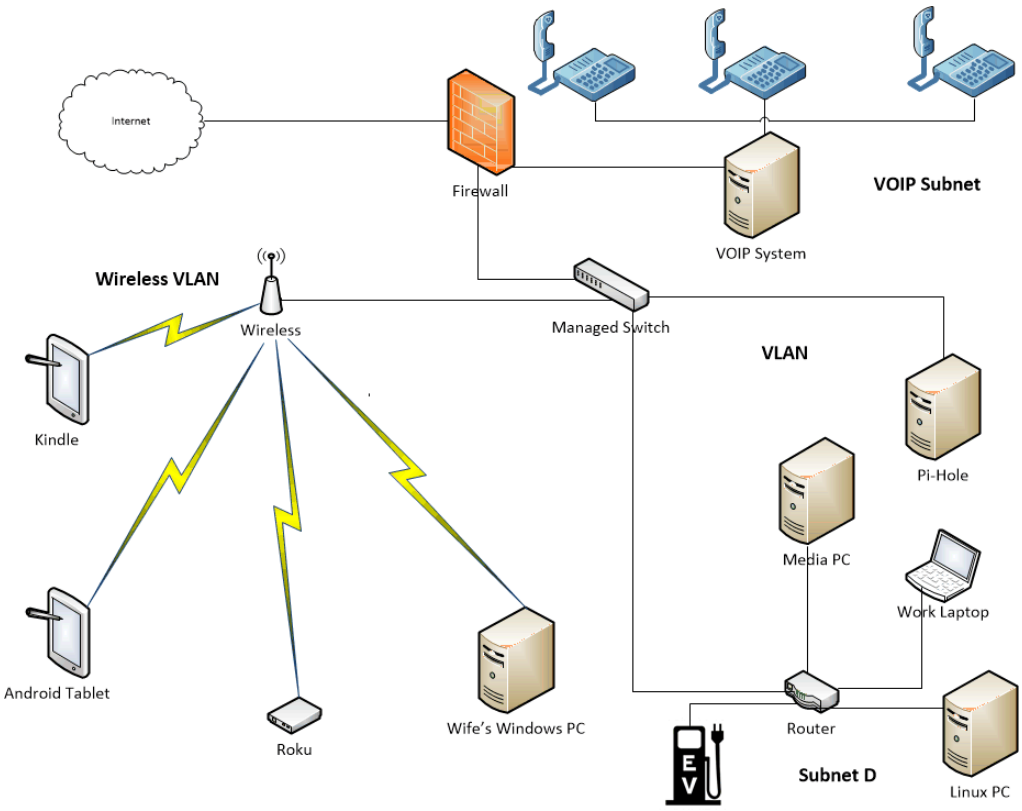
[16] https://www.slashgear.com/nest-home-security-hack-response-password-security-iot-06564817/

[17] http://techgenix.com/iot-thermostat-hacking/

[18] https://www.cnbc.com/2018/09/04/ex-nsa-privacy-expert-how-likely-your-amazon-echo-is-to-be-hacked.html

[19] https://www.youtube.com/watch?v=oo-hejIq3iQ

Figure 4



Two-Factor Authentication

Two-Factor Authentication, or 2FA, adds an extra layer of security for authenticating users to a system or device. The user will enter the username and password, then will be required to enter a piece of information to finally gain access to the system. 2FA can come from the following modalities:

- **Something you know:** This can be a number, such as a Personal Identification Number (PIN), or an answer to a secret question.
- **Something you have:** This would be something the user has in his/her possession. This could be a smartphone that receives a code to finalize the authentication process.
- **Something you are:** This can be a biometric system that can read fingerprints or eye retina patterns.

With 2FA, even if the credentials are stolen, the account is still protected because of the 2FA requirements needed to access a system. Some examples of 2FA include:

- Software (usable on a phone)
- Google Authenticator
- LastPass Authenticator
- Duo

Hardware devices used for 2FA are:

- Ledger Nano S
- Yubikey

If the home IoT device can support 2FA, this should be implemented to elevate the security of IoT devices and other home network devices.

For users who are interested in a simpler solution than configuring an open source firewall for protecting the younger members of the family against unwanted access to internet content, there are free services that can be used to filter internet content for the family. One such service is Open DNS[20] providing the ability to filter internet content by simply placing the “FamilyShield” [21]nameserver addresses (208.67.222.123 and 208.67.220.123) onto your home firewall/router DNS settings. Open DNS also provides a free account, with the ability to filter internet content coming into your home systems, as seen in figure 5.

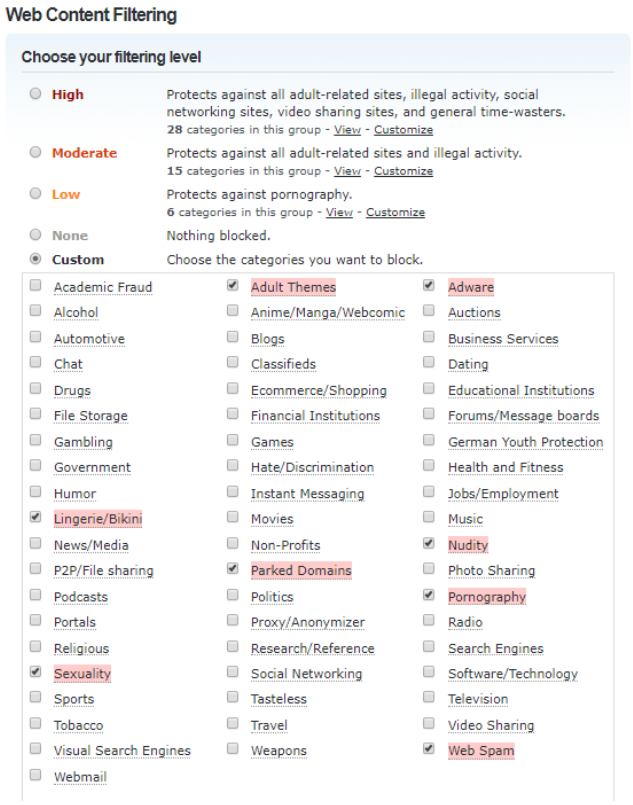


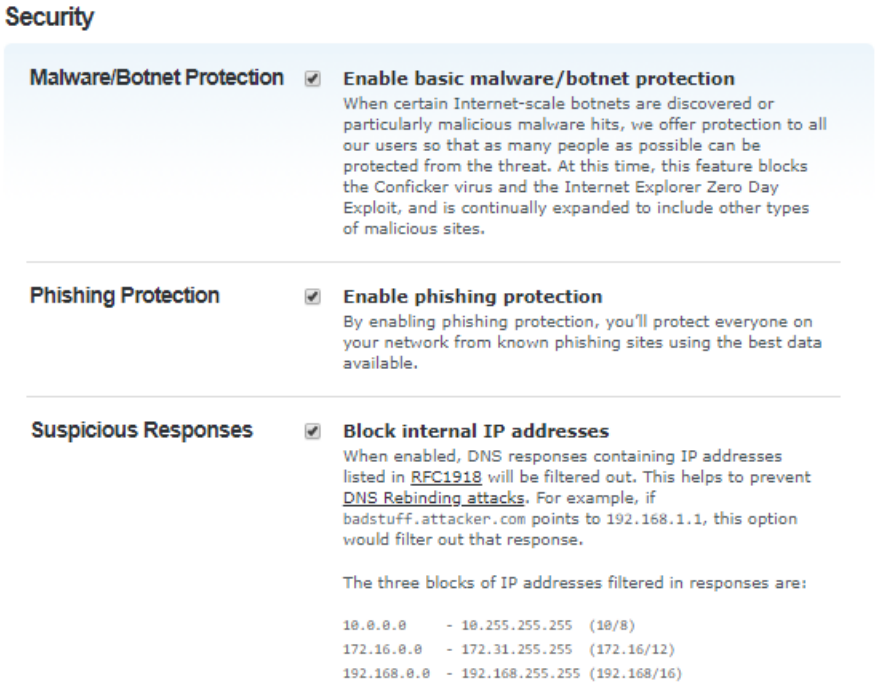
Figure 5

[20] https://signup.opendns.com/homefree/

[21] https://www.opendns.com/home-internet-security/

Further security settings can be made to protect against malware, botnets, and phishing as seen in figure 6 below:

Figure 6



Tracking and privacy

Adware is designed to display unwanted advertisements on PC systems, where it can redirect the user to advertising websites that collect and track information on PC surfing behavior. The table below is to demonstrate the differences between malware and adware. [22]

Table 1

Malware	Adware
A software program intentionally designed to cause damage to a system, computer or network	A software program designed to generate revenue by automatically generating online advertisements on the user's interface
A large range of malicious software	A type of malware
Can harm a computer or network in multiple ways depending on its intended target. Malware can destroy data, resources and cause network and configuration issues	Provides profit to the developer by generating online advertisement on the user's interface

Adware can also download advertising material/software that is often unwanted. Adware allows advertisers to spy on your browsing habits and to gather information including your IP address, and the webpages you query so that they can deliver advertisements based on query habits. There is no way to truly know what these adware programs collect from your system, but it may include logins, passwords and other personal information.[23] Furthermore, malevolent adware could possibly collect information on home IoT devices and the PC that manages them.

[22] https://pediaa.com/difference-between-malware-adware-and-spyware/

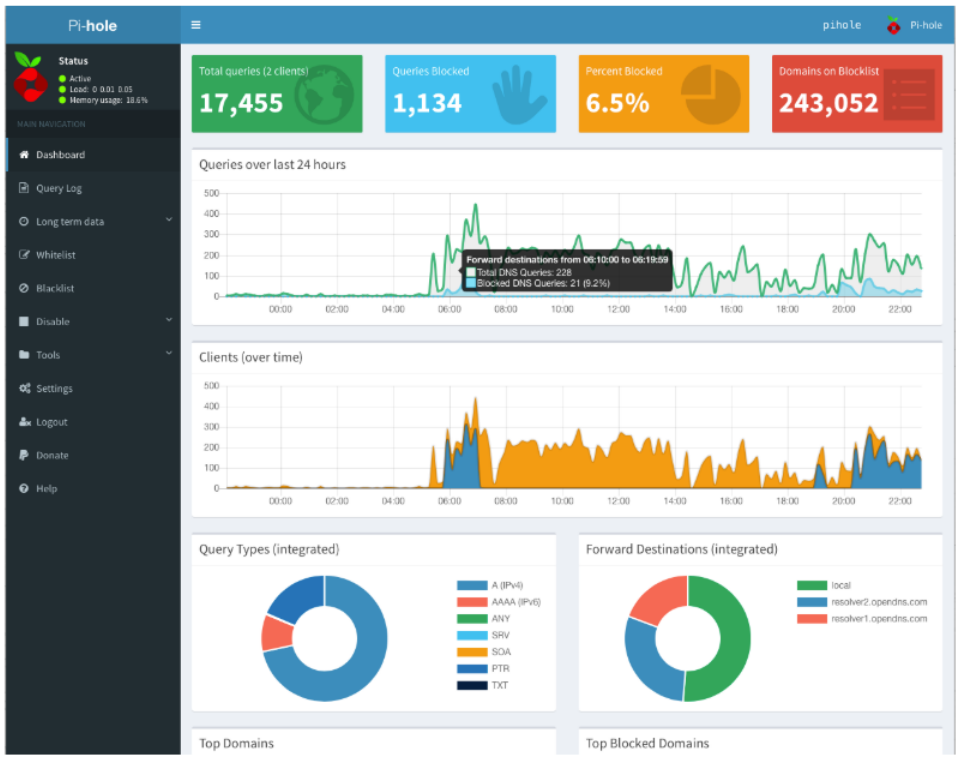
[23] http://www.besttechtips.org/why-is-adware-dangerous/

A tool to combat such unwanted software from installing on your PC or other smart devices on your network is Pi-hole. Pi-hole can be thought of as a network firewall for blocking advertisements and tracking domains for home PCs and other IoT devices, such as Smart TVs.[24] Pi-hole is a software that can be downloaded and installed on a dedicated PC on your home network.

Features provided by Pi-hole are:

- No client installed software is required to block ads
- Over 100,000 domains serving ads are blocked
- Ads can be blocked on Smart TVs and other devices
- Bandwidth improvements and overall network performance is increased
- A dashboard is provided allowing you to monitor blocking statistics via the Pi-hole webserver as seen in figure 7 below.

Figure 7



Making backups of your IoT devices, PC, and firewall/router is very important in case of hardware failures or disaster recovery. Backups should be made every time a configuration changes or an update is installed. Once a backup is made the homeowner should place those files in a secure location, which is preferably not accessible from the home network. One suggestion is to place the backups of all devices and systems of the home network onto a USB drive, then placing the USB drive in a secure location. If required to perform a system restore, the homeowner can readily access the USB drive to bring systems into operational mode.

[24] https://pi-hole.net/

Conclusion

Now more than ever, as homes become more and more sophisticated and connected, securing the home network is of utmost importance. Command and control of home systems, such as HVAC, freezers, refrigerators, and home Electrical Vehicle Charging stations present a very large attack surface to hackers who will attempt to introduce malevolent software, causing damage and loss to the homeowner. Furthermore, protection of privacy will require stronger security measures for the home network, where it has been reported one in three people will see the damaging effects on their privacy.[25]

About the author

Daniel Paillet is currently Cybersecurity Lead Architect within the Schneider Electric, Energy Management Business Unit. His background includes working in the US Department of Defense on various security projects. He has over 17 years of security experience in Information Technology, Operational Technology, Retail, Banking and Point-of-Sale. He holds the CISSP, CCSK, CEH and other agnostic and vendor specific certifications. His current role is to architect, improve, and develop secure solutions and offerings within Schneider Electric.

[25] https://www.helpnetsecurity.com/2019/06/13/iot-targeted-cyber-attacks/

Schneider Electric

Schneider Electric Industries SAS
35, rue Joseph Monier - CS 30323
F92506 Rueil-Malmaison Cedex

www.se.com

September 2019

998-20673868