Implementing and Maintaining a Secure Smart Home
Risks to Home Networks

The current reality of having many connected devices in the home has given rise to incidents of potential home network intrusions. In the first half of 2020, we detected over 10.6 billion suspicious connection attempts on routers' unavailable TCP ports. TCP port 23, in particular, had the most detections of suspicious connection attempts, with over 5.3 billion.

We believe that the requests on port 23 primarily came from internet of things (IoT) worm-related attacks rather than mere port scanning. Aside from port 23 being a known target of IoT worms, the requests are particularly suspicious because the connections were made on ports and services that are either closed by default or unavailable, as opposed to legitimate requests that are intentionally made through open connections. It appears that the connection attempts on the ports are non-specific targeting or probing-related activities on potential entry points.

Other noteworthy security events in home networks include the marked uptick in Secure Shell (SSH) brute-force login attempts. The trend has been observed since the onset of the Covid-19 pandemic. More employees are using remote access to their work, and malicious actors appear to be taking notice. These developments increase the risk of users in work-from-home arrangements, especially that connected devices (both for home and work) are in the same network.

Unavailable TCP port access attempts

It is typical for general detection mechanisms (including honeypots) to monitor open ports and services. Requests and attacks recorded on the services are used to identify attack trends. However, this method does not always detect potential attacks since connection requests for open services and ports are primarily legitimate.

For this analysis, we used deep packet inspection (DPI) in Trend Micro's consumer connected security to monitor external host connection requests in routers' unavailable ports. Connection requests are usually classified as port scans or attacks from non-specific targets. However, based on our telemetry, connection requests for the ports we monitor are different from each other. Not only are the top five source countries for each port's connection requests different, but so are the country rankings for the source IPs.

It should be noted that router connection attempts from external hosts are tackled here and not security events triggered by internal sources in the home network. Here are the TCP ports that we looked into:

- Port 21 - FTP control (command)
- Port 22 - SSH (SSH), secure logins, file transfers (scp, sftp) and port forwarding
- Port 23 - Telnet protocol—unencrypted text communications
- Port 80 - Hypertext Transfer Protocol (HTTP)
- Port 443 - Hypertext Transfer Protocol over TLS/SSL (HTTPS)
- Port 8080 - Alternative port for HTTP

The TCP transport layer allows the exchange of data and communication in several network ports that are associated with IP addresses and endpoints. Each port has underlying services (for example, email clients, web servers) that are at risk from attacks depending on several factors, including misconfigurations and ports left unmonitored and unprotected. Closing unused ports is like shutting the door on attackers. However, we found that many are suspiciously probing to access these entry points.

Unavailable port connection requests in 1H 2020

Here we show the trend in router events related to unavailable port connection attempts from January to June 2020. TCP port 23 had the most detections, including a significant increase in March. TCP port 23 is a known target by IoT worms and botnet malware. These access attempts are likely intended for non-specific target attacks or reconnaissance activities.

As seen in the figure below, there was a marked spike in connection requests for unavailable TCP port 443 in March and April. This is particularly notable because it is an unavailable service with a sudden increase in connection attempts. We speculate that this is due to a large number of attack attempts on web services and the TLS protocol.
According to Trend Micro’s telemetry, the access attempts on unavailable TCP port 23 in the first half of 2020 are closely aligned with the data for Telnet activity related to IoT worms during the same period. After all, the default port for Telnet client connections is 23. As a result, it is not far-fetched to conjecture that suspicious connection requests come from IoT worms.
In response to the Covid-19 pandemic, many companies have moved to work-from-home setups. This resulted in an influx of employees accessing remote services on the internet. Attackers, meanwhile, search for remotely accessible network services that are vulnerable to intrusion.

The figure above represents Telnet connection attempts. By June, the detections for the first half of the year reached a peak, where over 2 million events related to Telnet sessions were detected. Many connected devices still largely rely on Telnet for remote access capabilities.

It appears that malicious actors have ramped up their use of IoT worms via Telnet connections. Mirai variants, for instance, have been known to propagate in Telnet hosts and take advantage of default access credentials.

Attackers usually use IoT malware variants to perform brute-force attacks after scanning for open SSH and Telnet ports. They also find the latter particularly attractive since Telnet communication is unencrypted. IoT malware or botnet malware can also use exposed protocols to spread their infection to more routers. Attackers can listen in on the ports, snoop on credentials, and run commands for remote executions.
We also observed that brute-force login attempts, particularly through SSH, have also experienced significant growth. The use of weak credentials, such as default and easily guessed usernames and passwords, makes SSH and associated ports easy targets. SSH brute-force attacks are one of the preferred intrusion methods used by IoT botnets, ransomware, and other malware alike. Successful SSH brute-force attacks could lead to fileless cryptocurrency-mining attacks and seized control of victim servers, as also reported earlier this year.

Where are the access attempts coming from?
The source countries can be roughly divided into two groups. According to Trend Micro telemetry, for TCP ports 22 and 23, China held the top spot as the country with the most number of connection requests and source IPs. For TCP ports 21, 80, 443, and 8080, the United States ranked first.

The figures below refer to the number of connection requests (event counts) and the unique IPs we encountered. These are the source countries of probing attempts or possible attacks: that is to say, the direction that the attacks come from.

It is also worth mentioning that source countries for unavailable TCP port 443 had the highest number of unique IPs accessing the port, with over 847 million. Trailing behind was Telnet protocol port 23, with over 16 million. Note that some sources possibly route their attack attempts through proxies in other countries to evade detection.
Although this is only statistical information for possible intent, based on the logic of normal network connections, the huge increase in requests made to unavailable ports is suspicious. We will monitor and verify any changes to event counts and determine malicious sources for blacklisting.

**Security recommendations for home users of connected devices**

Owners of connected devices can implement network segmentation and isolate devices from public networks. To minimize the risk of data breach, owners should disable unnecessary services and components. Restricting traffic to specific ports can also be an added measure. In addition to following the aforementioned best practices on securing connected devices, users can look into the following:

- Patch device firmware to the latest versions. Always run the latest firmware to avoid attacks that exploit known vulnerabilities in services associated with unsecure ports.
- Use a firewall and an intrusion detection and prevention system. Use these systems to restrict suspicious activities and prevent attackers from accessing a device or network.
- Avoid the use of public Wi-Fi. Refrain from using public connections on devices used in home and corporate networks.
- Monitor outbound and lateral network traffic. Track the baseline of devices’ usage and normal traffic. Filter aberrant behavior that might be caused by rogue activities in the network.
- Configure systems. Use strong passwords and limit access to ports and services.

The **Trend Micro™ Home Network Security SDK** solutions block threats at the router level so that even the devices connected to a router stay protected against the threats that malware poses. An IoT scanning tool has been integrated into the Home Network Security solution and **HouseCall™ for Home Networks** scanner. HouseCall for Home Networks scans all of the devices connected to the home network to identify potential risks and offer suggestions about how to eliminate them. It works by using intelligent network scanning technology and finds device vulnerabilities.