Implementing and Maintaining a Secure Smart Home
TREND MICRO LEGAL DISCLAIMER
The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Contents

4
Risks to Home Networks

10
Securing Home Routers

12
Comprehensive Security Solutions for Home Routers

15
Conclusion
Trend Micro predicted that threats to Internet of Things (IoT) devices would go mainstream in 2017, ushering in an era of new attacks on smart devices for both consumers and industrial environments.¹ The appearance of the Mirai botnet in 2016 lent credence to this prediction: It let criminals launch massive and widespread attacks by taking advantage of vulnerable IoT devices — including routers, closed circuit video cameras and digital video recorders — found on many home networks.²

The Mirai botnet powered numerous high-profile attacks against both Linux® and Windows®-based systems, confirming the vulnerability of common IoT devices to malicious abuse. Compromised IoT devices have also affected businesses by transforming them into proxies when credential stuffing attacks made use of Netgear routers.³

According to a 2017 report by Pwnie Express,⁴ 92 percent of IT professionals believed that connected device threats would become a major security issue in 2017. Eighty-four percent said Mirai changed their perception of threats against IoT devices, but 66 percent of respondents also said they either did not know or weren’t sure how to check their devices for signs of that botnet. Even more troubling, only 22 percent of the respondents claimed to monitor connected devices in the workplace.

With the scale of home networks becoming exceedingly similar to that of small offices, management and security across devices have become more important than ever, especially for oft-overlooked routers.

Risks to Home Networks

The number of connected home devices continues to increase and diversify at a rapid pace, going far beyond computers, mobile phones and tablets. In general, the increasing number of connected devices leads to greater convenience and efficiency, but the risks may soon begin to overshadow the benefits.

Trend Micro has shown the risk of attacks on a fully connected smart home through a variety of scenarios.\(^5\) A poorly configured wireless home network and weak passwords can give attackers the advantage. Failures by IoT device manufacturers to release firmware updates can inadvertently put the devices that they sell at risk as well. Attackers can exploit vulnerable devices to spy on or steal from unsuspecting victims.

Data gathered from Trend Micro Smart Home Network™ logs shows that between 10 percent and 20 percent of homes already have compromised devices. Around 40 percent of routers allow visits to malicious websites every week.

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Source</th>
<th>Percentage of Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United States</td>
<td>28%</td>
</tr>
<tr>
<td>2</td>
<td>China</td>
<td>7%</td>
</tr>
<tr>
<td>3</td>
<td>United Kingdom</td>
<td>7%</td>
</tr>
<tr>
<td>4</td>
<td>Hong Kong</td>
<td>5%</td>
</tr>
<tr>
<td>5</td>
<td>Canada</td>
<td>5%</td>
</tr>
<tr>
<td>6</td>
<td>Australia</td>
<td>4%</td>
</tr>
<tr>
<td>7</td>
<td>Sweden</td>
<td>4%</td>
</tr>
<tr>
<td>8</td>
<td>Netherlands</td>
<td>4%</td>
</tr>
<tr>
<td>9</td>
<td>Taiwan</td>
<td>3%</td>
</tr>
<tr>
<td>10</td>
<td>Russia</td>
<td>3%</td>
</tr>
</tbody>
</table>

Table 1. Top 10 source countries for router attacks during the first half of 2017

---

Home routers observed 28 percent of network attacks with the Smart Home Network enabled in the U.S. The total network intrusion attacks totaled around 1.8 million attacks just during the first half of 2017. The top 10 source countries for router attacks, listed in Table 1, account for approximately 70 percent of incidents detected globally in smart homes by Trend Micro, indicating that smart home security issues constitute a global threat.6

A connected device, once compromised, may also carry out malicious activities such as scanning and discovering other vulnerable devices, performing distributed denial-of-service (DDoS) attacks, and bitcoin mining. (Trend Micro’s blog article “Home Routers: Mitigating Attacks that can Turn them to Zombies” provides more details.7)

Large-Scale Attacks on Connected Devices

The 1.8 million attacks on home devices observed during the first half of 2017 consisted of both inbound and outbound attacks. Inbound attacks target smart devices on a home network via the internet (internet to home network). Outbound attacks (home network to internet) result when the attacker gains control of network devices through an inbound attack and then later uses them to breach and attack other devices elsewhere on the internet.

<table>
<thead>
<tr>
<th>Inbound Attack Type</th>
<th>Event Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Brute Force Login</td>
<td>140,054</td>
</tr>
<tr>
<td>WEB Brute Force Login -1</td>
<td>60,092</td>
</tr>
<tr>
<td>Netcore Router Backdoor Access</td>
<td>40,757</td>
</tr>
<tr>
<td>WEB-CLIENT Suspicious HTML Iframe Tag -4</td>
<td>32,767</td>
</tr>
<tr>
<td>WEB-CLIENT WScript.Shell Remote Code Execution -1</td>
<td>16,382</td>
</tr>
<tr>
<td>RDP Brute Force Login</td>
<td>9,758</td>
</tr>
<tr>
<td>WEB-CLIENT Generic Javascript Obfuscation -6</td>
<td>8,127</td>
</tr>
<tr>
<td>WEB-CLIENT Javascript Obfuscation in Exploit Kits - 62</td>
<td>7,469</td>
</tr>
<tr>
<td>WEB-CLIENT Javascript Obfuscation in Exploit Kits - 65</td>
<td>4,642</td>
</tr>
<tr>
<td>WEB-CLIENT Javascript Obfuscation in Exploit Kits – 32</td>
<td>4,343</td>
</tr>
</tbody>
</table>

Table 2. Top 10 inbound attacks during the first half of 2017


Table 2 shows the top 10 inbound attack types detected by Trend Micro Smart Home Network. Most events involved brute force login attacks (or default password logins).

A brute force login attack (or default password login) attempts to discover a password by trying out likely combinations of letters, numbers and symbols systematically. (Trend Micro has found this method of attack difficult to detect.) After finding a password match, the attacker can fully control the router or connected device and deploy it maliciously. Mirai used a brute force login attack with alarming success.8

<table>
<thead>
<tr>
<th>Outbound Attack Type</th>
<th>Event Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Amplification Attack</td>
<td>629,094</td>
</tr>
<tr>
<td>IIS HTTP.sys DoS (CVE-2015-1635)</td>
<td>414,102</td>
</tr>
<tr>
<td>IMAP Command B.O.</td>
<td>152,818</td>
</tr>
<tr>
<td>HTTP Negative Content-Length B.O.</td>
<td>50,257</td>
</tr>
<tr>
<td>ICMP BlackNurse Attack</td>
<td>48,621</td>
</tr>
<tr>
<td>SSH Brute Force Login</td>
<td>29,463</td>
</tr>
<tr>
<td>TP-LINK Router DoS</td>
<td>25,000</td>
</tr>
<tr>
<td>Server Service Remote Code Execution</td>
<td>20,629</td>
</tr>
<tr>
<td>NULL-Byte Injection</td>
<td>16,258</td>
</tr>
</tbody>
</table>

Table 3. Top 10 outbound attacks during the first half of 2017

Table 3 shows the top 10 outbound attack types detected by Trend Micro Smart Home Network. Trend Micro classifies nearly 80 percent of router attacks as outbound attacks.9 Outbound attacks must first successfully compromise or infect the home devices before delivering the final attack payload.

Trend Micro Smart Home Network log data shows that attackers have used Domain Name System (DNS) amplification attacks, or DNS reflection denial-of-service (DoS) attacks, most often, with more than 600,000 events recorded. A typical DNS reflection DoS attack proves difficult to trace due to spoofing of the source IP address. As an effect of the attack, targeted devices are flooded with packets, which are either replies from the DNS server or error messages going back to the victimized “sender.”10

---


<table>
<thead>
<tr>
<th>Noteworthy Events</th>
<th>Event Count</th>
<th>Average Events per Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Amplification Attack</td>
<td>629,098</td>
<td>343</td>
</tr>
<tr>
<td>Bitcoin Mining</td>
<td>481,682</td>
<td>89</td>
</tr>
<tr>
<td>IIS HTTP.sys DoS</td>
<td>414,110</td>
<td>139</td>
</tr>
<tr>
<td>Brute force Login</td>
<td>256,804</td>
<td>35</td>
</tr>
<tr>
<td>IMAP Command B.O.</td>
<td>152,829</td>
<td>44</td>
</tr>
<tr>
<td>Telnet Default Password Login</td>
<td>128,520</td>
<td>208</td>
</tr>
<tr>
<td>ICMP BlackNurse Attack</td>
<td>50,533</td>
<td>9</td>
</tr>
<tr>
<td>HTTP Negative Content-Length B.O.</td>
<td>50,260</td>
<td>28</td>
</tr>
<tr>
<td>Netcore Router Backdoor Access</td>
<td>48,114</td>
<td>156</td>
</tr>
</tbody>
</table>

Table 4. Bidirectional network events during the first half of 2017

Table 4 shows the ranking of all noteworthy events, event counts, devices and average events per device. The noteworthy events consist of inbound and outbound attacks, as well as intrusion prevention system (IPS) security events triggered by IPS rules. The IPS security events tracked during the first half of 2017 include greynet events (40 percent), which refer to unauthorized applications running on corporate networks. Note that greynet applications are not necessarily malicious and may oftentimes include potentially unwanted programs such as adware or other grayware.

**Mining for Bitcoin With IoT Devices**

Trend Micro Smart Home Network logs have shown that bitcoin mining events constitute just over 10 percent of the total IPS events for the first half of 2017. This computationally intensive task requires significant resources from dedicated processors, graphics cards and other hardware. To avoid the high electricity costs associated with generating the cryptocurrency, criminals now seek to create an army of computers, home routers and IoT devices.\(^\text{11}\)

Figure 1. IPS event distribution for the first half of 2017

Figure 2. IPS event distribution comparison between January 2017 and June 2017
Trend Micro researchers believe that bitcoin mining increased significantly during the months of May and June when the cryptocurrency reached a value of US$3,000. Most cryptocurrency activities took place on computers running Microsoft Windows®, but also affected these devices:

- Apple hardware running MacOS® and iOS (iPhone 4 to iPhone 7)
- Devices running the Ubuntu® operating system (OS), a derivative of the Debian Linux® OS
- Home routers
- Environment-monitoring devices used in data centers
- Smart TVs and mobile devices running Android™
- IP cameras
- Print servers
- Gaming consoles

After taking control of a target, some attackers even patch the security gap that they used to prevent others from gaining control of their assets. People who spend little time administering devices like IP cameras may never notice that their gadgets have started generating currency for a total stranger.

These types of attacks on IoT devices will become more prevalent if the value of cryptocurrencies like bitcoin and ethereum continues to rise. By 2022, bitcoin prices may climb to US$25,000, and possibly rise to US$50,000 by 2027, making bitcoin mining a highly lucrative business.

Compromised devices may also trigger these events:

- MS IIS DoS (CVE-2015-1635) - Microsoft Windows HTTP.sys integer overflow vulnerability
- Telnet default password logins
- Brute force logins (RDP, WEB, SSH)
- IMAP command buffer overflows

---

Securing Home Routers

IoT devices usually depend on a home router to connect to the internet. The design of most home routers does not prioritize security, however, leaving connected devices vulnerable to many exploits, DDoS attacks, backdoor threats, etc. Unsecured default configurations and other firmware flaws also add further risks to many home routers. Attackers can easily run a quick search of routers’ predefined credentials to infiltrate and take command of these devices.

A vulnerable home router can eventually put an entire home network at risk, including not only the actual devices, but also all of their stored data, even those in the cloud. Criminals focus on home routers for information theft to generate quick bucks.

Underground markets on the dark web rent out bots offering user data for DDoS attacks for substantial profits. Renting 100 bots from the Chinese underground would cost around US$24 in 2015, while renting 100-150 bots per day from the French underground would cost around €95 (or US$102.19).16

Future Home Network Attacks

People who connect to the internet from their homes usually connect via network address translation (NAT), the process by which a firewall assigns a public address to a computer inside a home network. Connecting via NAT offers some security benefits, but external attackers can still directly access connected devices in these situations:

- Transparent mode: when a public IP gets assigned to a connected home device
- Port forwarding (also known as port mapping): when the configuration of the router opens up certain ports so that programs can get inside (this sort of “hole” in a home router can allow for remote access to network-attached storage or NAS servers and IP cameras)
- Hardware and software vulnerabilities: attackers can take advantage of known flaws to infiltrate the network

Attacks against home networks via routers generally only occur in the situations described above. Most attackers cannot reach devices behind a NAT, because all NAT routers inherently function as effective firewalls.

Attackers generally compromise connected devices like smartphones, tablets and smart TVs through these entry points:

- The victim visits a dangerous website and downloads malicious files.
- The victim opens a malicious attachment in an email message from a stranger.
- The victim keeps the default password or sets a weak password when setting up a router.
- The victim uses outdated software or firmware.
- System infections spread from one local area network (LAN) to another.

Once infected by malicious software, the affected devices can eventually join a “zombie army” to attack servers or other devices.
Comprehensive Security Solutions for Home Routers

Trend Micro has a solution to make home routers protect home networks by stopping direct attacks and other malicious activities, as well as block inappropriate or dangerous websites.

Trend Micro Smart Home Network

The Trend Micro Smart Home Network (SHN) provides an embedded network security solution to protect against cyberattacks and network access management for all devices connected to a home network. Many leading home router vendors have already adopted this solution and deployed it to more than 1 million households worldwide. Based on Trend Micro’s rich threat research experience and industry-leading deep packet inspection (DPI) technology, SHN offers intelligent quality of service (iQoS), parental controls, network security and more.

Figure 3. Trend Micro Smart Home Network solution
For home router vendors who have not developed their own management consoles, Trend Micro provides a mobile app for customers to manage SHN from their favorite mobile devices.

Building a Secure Home Network

SHN follows these basic tenets:

Device Identification (Device-ID) and Application Identification (Application-ID)

Using both Device Identification (Device-ID) and Application Identification (Application-ID), SHN provides visibility across the entire home network.

Device-ID identifies around 3,800 device types, including smartphones, tablets and smart TVs. Application-ID identifies more than 2,200 application behaviors, including instant messaging apps, peer-to-peer (P2P) networks and file-sharing services, among many others.

iQoS makes use of Device-ID and Application-ID to help improve internet traffic management capabilities through enhanced application and device identification methods.

Intelligent Quality of Service (iQoS)

Intelligent Quality of Service (iQoS) helps improve internet traffic management capabilities through better application and device identification, bandwidth allocation and traffic prioritization techniques. iQoS resolves network traffic congestion due to limited internet bandwidth or heavy competition for bandwidth.

iQoS has a two-tier bandwidth management system: by Application-ID and Device-ID. Application-ID sets priorities based on traffic type and assigns a precise amount of bandwidth to streaming applications based on their resolution and bandwidth needs. For example, online gaming applications require low network latency and thus have higher priority. Paid services like Netflix® and Hulu® get higher priority over free services.

Next, Device-ID prioritizes traffic based on device types, giving the user total control over assigning bandwidth priority to all applications. For instance, they can rank devices according to screen size and giving smaller devices, like smartwatches, the least amount of bandwidth.

Parental Control

Because SHN can identify and block network packets that belong to specific applications, the Parental Control provides powerful capabilities for protecting children who use the internet with these specific features:
• Monitor or block what kids do online
• Set internet time limits according to user profiles in real time
• Easily block websites by category
• Prevent kids from seeing inappropriate content

Network Security

With a built-in DPI engine, SHN can identify and block attacks before those packets reach vulnerable IoT-enabled devices, mobile devices and computers. With malicious traffic blocked by the home gateway, virtual patching is possible.

This feature also uses the IoT Reputation Service (IoTRS) to block suspicious peers in the first place. Machine learning technology detects abnormal behavior in devices connected to the home network.

SHN puts a three-step process in place to deal with the “before, during and after” stages of an infection:
1. A router health check provides system configuration guidelines, such as password strength.
2. Vulnerability and malicious website protection identifies and blocks exploitation attacks before the attacking packets can reach vulnerable devices.
3. Infection mitigation prevents infected devices from sending personal information or infection status updates outside the home network.

On-the-Go

SHN also offers a mobile app to control network access of mobile devices that belong to children even if they venture away from the home network.

Cloud Data Analysis

Trend Micro provides quarterly statistics to home router vendors via the Trend Micro™ Smart Protection Network™.

The Smart Protection Network uses a global network of threat intelligence sensors to update email, web and file reputation databases in the cloud continuously, identifying and blocking threats in real time before they can cause harm.

The Smart Protection Network cloud data mining framework collects more than 15TB of threat data each day through a worldwide network of honeypots, submissions, feedback loops, web crawling technologies, customers and partners, and Trend Micro’s own forward-looking threat researchers.
Conclusion

The sophistication of connected home requires new approaches to cybersecurity. No longer do only a few gadgets – a PC here, a smartphone there – connect to the internet. Instead, wide sections of home infrastructure now connect through a home router. Keeping intruders from gaining control over a home camera system or kitchen appliance requires more than just installing security software on every single thing.

Attackers have already compromised at least 10 percent of all households to date, with a little over 40 percent of routers accessing malicious websites on a weekly basis. Compromised devices can continuously access malicious sites, commit DDoS attacks and participate in bitcoin mining.

Trend Micro has observed that despite current security measures in place for home routers, attackers can still use port-forwarding as a means of entry. Hackers can even use compromised IoT devices to target large enterprises. The same IoT resources used for clandestine bitcoin mining can also attack enterprise networks with ransomware and DDoS attacks.

Protecting home IoT devices does truly make a difference in maintaining global information security.
TREND MICRO™
Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers’ and partners’ needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.