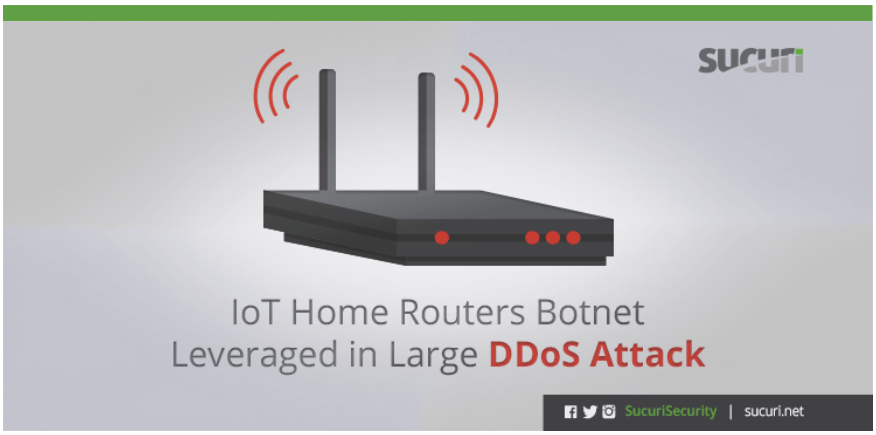
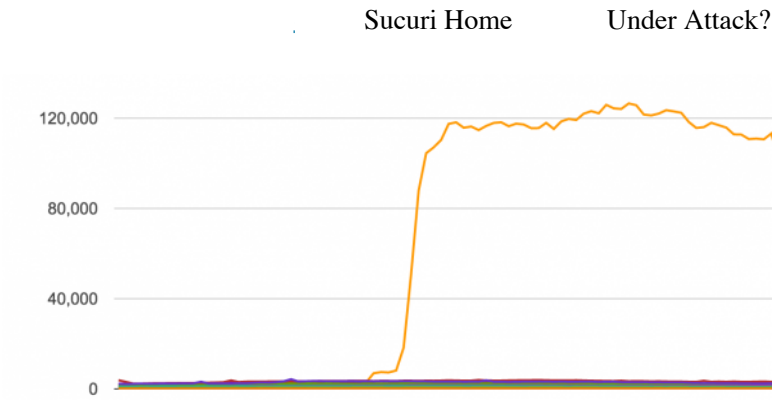


IoT Home Router Botnet Leveraged in Large DDoS Attack

SEPTEMBER 1, 2016 DANIEL CID

We have been monitoring a large-scale Layer 7 HTTPS flood attack (i.e., application level DDoS) against a customer over the past few weeks. It is being distributed across **47,000 IP addresses** and has been pushing over **120,000 HTTPS requests per second** (RPS) to the website.

Unlike volumetric attacks that target the network link (measured in bits per second), application-based attacks are designed to target the application and web server resources (measured in requests per second).



Beginning of large-scale Layer-7 DDoS

This customer came to us after trying to mitigate the DDoS attack using Amazon (AWS), Google (GCE), and other cloud-based auto-scaling solutions. At this scale, most load balancers and VPS cloud instances cannot sustain this level of traffic.

For this website owner, the attack was big enough to **disable multiple web servers** and quickly exhaust their available bandwidth. This was further exasperated through the use of **HTTPS requests**, which is more CPU intensive because of the TLS/SSL handshake.

DDoS Botnets

An application-level DDoS attack is not the most interesting aspect of this story.

We recently shared a post on a CCTV-based botnet used to initiate large-scale application-level DDoS attacks against websites. We also shared insights into how unsuspecting WordPress sites can form a malicious botnet to perform DDoS attacks via the XMLRPC feature. In both cases, attackers gain enough **computing**

Categories

- Ask Sucuri
- Drupal Security
- Ecommerce Security
- Joomla Security
- Magento Security
- Security Advisory
- Security Education
- Sucuri Updates
- Vulnerability Disclosure
- Website Firewall
- Website Malware Infections
- Website Pharma Hack
- Website Security
- Website SEO Spam
- WordPress Security

victim to add more computing and networking power to fight off attacks, which is highly unrealistic for most website owners.

This website owner tried several options to combat the DDoS attack. They tried the AWS auto-scaling service but reached a point where the cost was too great. They were paying large sums of money as the attack grew. For the attacker, using a botnet means they pay nothing to succeed. The victim has to pay for additional servers and bandwidth, while attackers get it for free using their malicious botnets.

That resource and cost imbalance makes DDoS mitigation tricky for most website owners.

Analyzing the 120K Layer 7 DDoS Attack

If you recall our CCTV-based botnet, the attackers had compromised 25,000 different IoT CCTV devices for their DDoS campaign. They were also generating an excess of **35,000 HTTP RPS** against the site. In contrast, the attack we are analyzing today is **four times (x4) the size** of the CCTV-based attack. How did they achieve this?

In this case, attackers were making use of multiple botnets. They either rent or trade with other attackers distributed across 47,071 + IP addresses. By fingerprinting the IPs, we were able to profile 3 different botnets:

2. IoT Home Routers Botnet (new)
3. Compromised web servers coming from data centers (very common)

This new distribution allowed the attacker to generate a massive number of requests per second without affecting the operation of the infected devices. Under this configuration, the devices would only need to generate a few requests per second – well within their means.

IoT Home Router Botnet

Perhaps the most interesting bit of data for us (being that we're very familiar with CCTV and compromised web server botnets) was the introduction of the home router botnet. While we have seen routers being used maliciously in the past, we have never seen them used at this scale.

In this case, home routers made up 25% of the IP addresses, resulting in about **11,767 compromised routers**. We were able to fingerprint the makeup of the home routers and it came down to eight major router brands being used in the campaign.

Routers being targeted by attackers is nothing new. Over the years there has been a lot of discussion in the community over the inherent risks they introduce to networks, along with other "plug-and-forget" devices (ex. WAPs,

malware, and even vigilante malware (e.g., Linux.Wifatch).

While it has always been a possibility, seeing a DDoS rolled into one large-scale home router botnet was new to us.

Huawei Routers

The largest number of routers being exploited came from Huawei-based routers. They varied between versions: HG8245H, HG658d, HG531, etc.

We identified at least **6,015 compromised devices** (51%). It's difficult to know exactly how they were exploited, but a good place to start is with the brand's security advisory page.

HG531 router
RouterOS login page

HG658d router
RouterOS login page

HG8245H router
RouterOS login page

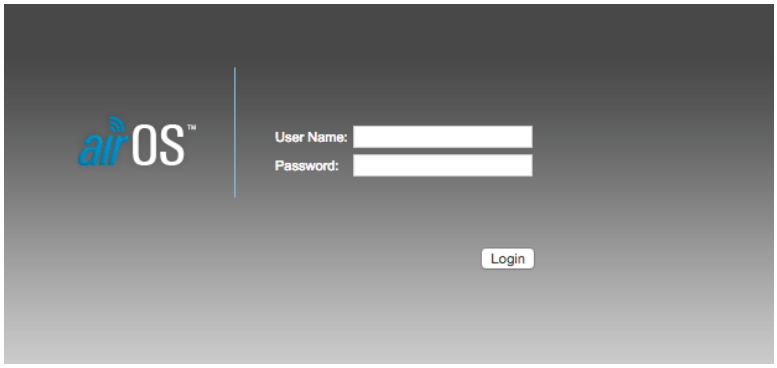
RouterOS Devices

Mikro RouterOS was the second most popular router behind this attack with **2,119 devices** (18%).

RouterOS login page

AirOS Routers

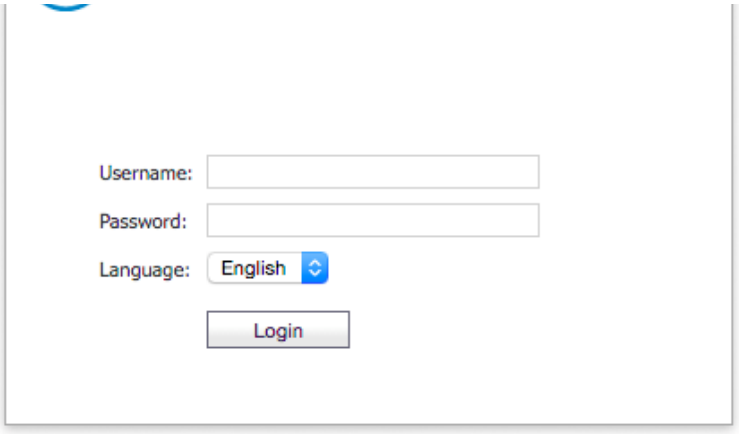
Third place goes to AirOS, a Ubiquiti Networks device with **245 home routers.**



RouterOS login page

Others

These were not the only routers being used. The rest were distributed across a number of different providers including NuCom 11N Wireless Routers, Dell SonicWalls, VodaFone, Netgear, and Cisco-IOS routers.

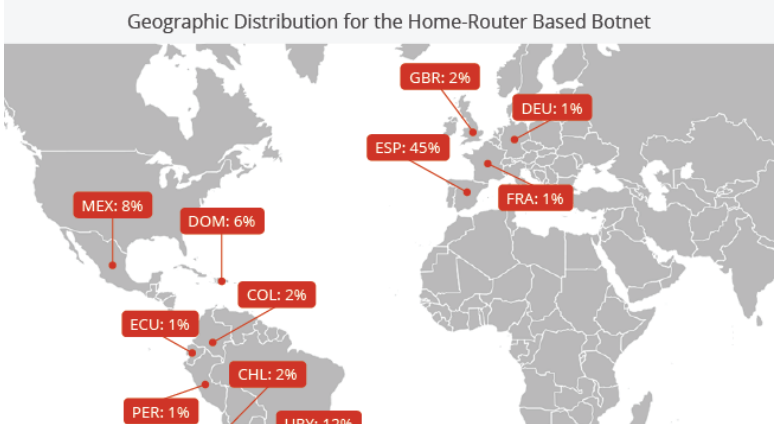


Dell SonicWALL router login page

IoT Home Router Botnet Diversity

A key requirement for the success of these attacks is diversity. This includes geographic distribution, ASN, ISP, and IP networks. This home router botnet had solid diversity with a heavy focus on Spanish-speaking countries (e.g., Spain, Uruguay, and Mexico). The more diverse the networks are, the harder it is for the victim site to isolate the attack and block one or two networks.

Here is the geographical distribution for the home router botnet:



The attack came from **175** /8 networks and **5,000** /16 distinct networks.

The most misused /24 blocks were:

Most Misused /24 Blocks	
1.	189.219.122.0/24 - *Television Internacional, MX*
2.	85.203.32.0/24 - *ARETI-AS , GB*
3.	31.4.241.0/24 – *VODAFONE, ES*
4.	190.233.151.0/24 – *Telefonica del Peru*
5.	212.225.226.0/24 – *PROCONO-AS*
6.	80.58.250.0/24 – *TELEFONICA_DE_ESPANA*
7.	90.174.4.0/24 – *UNI2*
8.	5.254.65.0/24 – *VOXILITY*
9.	213.143.50.0/24 – *UNI2*
10.	91.109.30.0/24 – *LEASEWEB*

In terms of ASNs, these were the top 10 providers:

Top 10 ASN Providers
17% - TELEFONICA_DE_ESPANA, ES
12% - Administracion Nacional de Telecomunicaciones, UY
7% - UNI2-AS, ES
7% - JAZZNET Global Spanish ISP, ES
6% - Compañía Dominicana de Teléfonos, C. por A. – CODETEL, DO
6% - ONO-AS Cableuropa – ONO, ES
5% - Uninet S.A. de C.V., MX
2% - VODAFONE_ES, ES
2% - CANTV Servicios, Venezuela, VE
1% - Telecom Argentina S.A., AR
1% - Telefonica de Argentina, AR
1% - CABLEVISION S.A., AR
1% - Telefonica del Peru S.A.A., PE
1% - CORPORACION NACIONAL DE TELECOMUNICACIONES – CNT EP, EC
1% - Telmex Colombia S.A., CO
1% - Mega Cable, S.A. de C.V., MX

IoT Botnets on the Rise

surface of what we can expect in the future. As more devices become part of the IoT ecosystem, the greater the threat becomes. We know that human behavior tends to favor convenience over security when it comes to maintaining their devices.

In conducting our research, we made attempts to identify the attack vectors used in the exploit but fell short due to limited access. We were able to locate a number of public exploits, and many of the **devices have not been patched**. I would assume that a large number were likely abused through the use of **weak or default router passwords**.

If you want to check if your router is compromised, F-Secure has a great online scanner that remotely checks for any external issues. While it won't address all issues, it will look for things like potential DNS-hijacking.

A great resource to help walk you through the process of securing your home router is: http://routersecurity.org/

If your website is experiencing availability issues (meaning it continues to go down or your web servers are being exhausted) you might benefit from leveraging a cloud-based website application firewall that specializes in DDoS attacks.

TAGS: Botnet, DDoS, HTTP/HTTPS, Layer-7

ABOUT DANIEL CID

Daniel B. Cid is the Founder & CTO of Sucuri and also the founder of the open source project - OSSEC HIDS. His interests range from intrusion detection, log analysis (log-based intrusion detection), web-based malware research and secure development. You can find more about Daniel on his site dcid.me or on Twitter: @danielcid