CENTURYLINK 2018 THREAT REPORT

CenturyLink®

Executive Summary:

As cyber threats proliferate, businesses, governments and consumers often seek to find the silver bullet for cyber security issues. With so many differing viewpoints of the threat landscape, the task of identifying actionable intelligence, while prioritizing who and what to protect, is a difficult one. Meanwhile, the growth of cyber threats continues to be explosive, and the cost to protect businesses and consumers is on the rise.

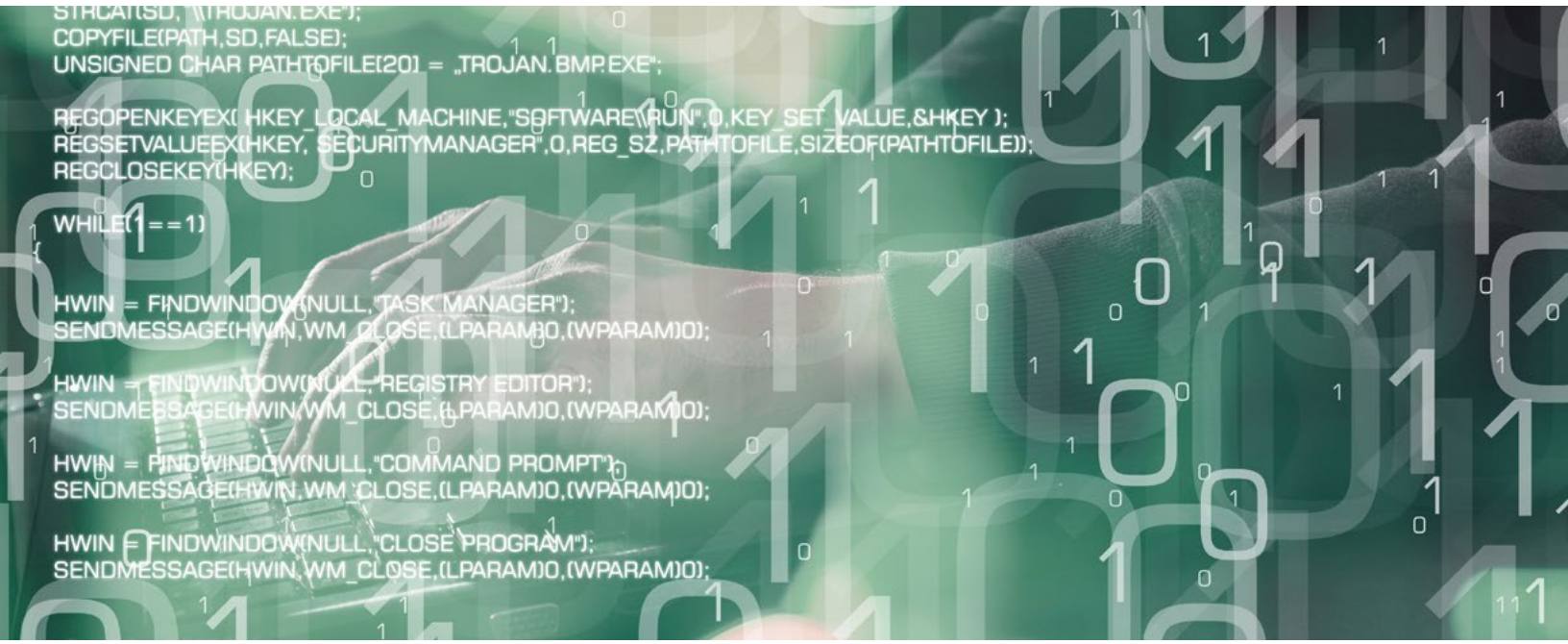
No one is completely immune to today's – or tomorrow's – cyber threats. We can relate to the business challenges organizations face in our connected world. Like our customers, CenturyLink works tirelessly to protect itself from the evolving and increasingly sophisticated, malicious operators looking to exploit any weakness.

In this report, as we do regularly for our customers, fellow security researchers and other leading ISPs, we are offering the IT community the same unique insights we use to protect ourselves and our customers with the goal of regaining the upper hand from cybercriminals. This intelligence varies from other industry threat reports because it is based exclusively on what CenturyLink® Threat Research Labs sees across the CenturyLink global backbone.

The report opens with our insights around the sources of global malicious traffic and the victims they target. We then breakdown the components of attack traffic by identifying the origins of command and control servers (C2s) and the bots they control, along with a review of bot attack targets compared to those of all threats we monitor. Finally, we present an exclusive deep dive into the evolution and presiding trends with respect to DDoS IoT botnets.

CenturyLink®

Table of Contents



CenturyLink®

Understanding the **Global Threat** Landscape Puzzle.

Our Unique View of the World

More than 4 billion people – essentially half the world's population – now have access to the internet. Among the petabytes of data traversing our global network backbone, **CenturyLink Threat Research Labs tracked an average of 195,000 threats per day in 2017, impacting, on average, 104 million unique targets daily.** For the purposes of this report, "targets" refers to servers, computers, handheld or internet-connected (IoT) devices owned by businesses, government entities and individual consumers. The term "victims" is used to refer to those entities with compromised servers, computers and devices being used to attack the targets described above.

We look first at the attackers. As reported in previous editions of our threat report (see Attack of the Things and How the Grinch Stole IoT), geographies with strong or rapidly growing IT networks and infrastructure continue to be the primary source for cybercriminal activity. At a recent cybersecurity summit hosted in Denver, Colorado, speakers indicated that the emphasis on STEM (science, technology, engineering and math) training in rapidly developing countries has added to the proliferation of bad actors. However, the United States, Russia and China hold the lead as the three most common points of origin for malicious internet activities.

For malicious traffic by country of origin, we've broken the data down by the top 10 countries generating traffic from a global perspective and provided additional breakouts for malicious traffic origins within Europe, Latin America and Asia Pacific.

Malicious Traffic

by Country of Origin Full Year 2017

Top 10 Countries Globally

1. **United States**
2. **Russia**
3. **China**
4. **Brazil**
5. **Ukraine**
6. **Germany**
7. **France**
8. **Netherlands**
9. **Turkey**
10. **United Kingdom**

Source: CenturyLink Threat Research Labs, Full Year 2017

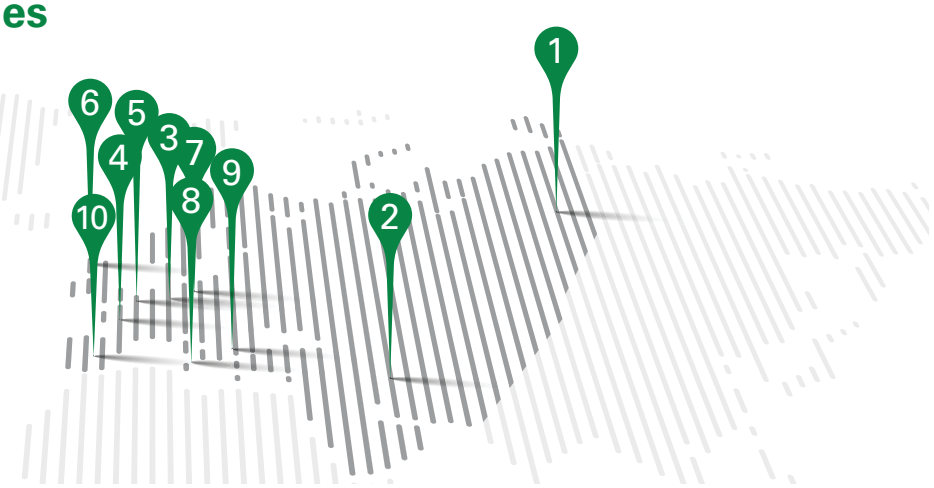
CenturyLink®

Malicious Traffic

by Country of Origin Full Year 2017

Top 10 European Countries

1. Russia
2. Ukraine
3. Germany
4. France
5. Netherlands
6. United Kingdom
7. Poland
8. Italy
9. Romania
10. Spain



Top 5 Latin American Countries

1. Brazil
2. Argentina
3. Mexico
4. Chile
5. Colombia

Top 5 Asia Pacific Countries

1. China
2. South Korea
3. Vietnam
4. India
5. Australia

CenturyLink®

Source: CenturyLink Threat Research Labs, Full Year 2017

Next, we will look at a few of the different varieties of the malicious activity CenturyLink monitors, starting at the top of the heirarchy with the C2 systems directing the attacks.

Traffic between a network and any C2 server is a powerful risk indicator that a vulnerable and potentially compromised host exists. Depending on the network's topology, this compromised host may also give the attacker access to the devices behind the security mechanisms in place. Tracking C2 data reveals victim hotspots and activity hubs favored by malicious actors.

C2s
by Country of Origin Full Year 2017

Top 10 Countries Globally

1. **United States**
2. **Russia**
3. **Ukraine**
4. **China**
5. **Germany**
6. **Netherlands**
7. **France**
8. **United Kingdom**
9. **Brazil**
10. **Canada**

Top 10 European Countries

1. **Russia**
2. **Ukraine**
3. **Germany**
4. **Netherlands**
5. **France**
6. **United Kingdom**
7. **Italy**
8. **Spain**
9. **Poland**
10. **Turkey**

Source: CenturyLink Threat Research Labs, Full Year 2017

CenturyLink®

C2s
by Country of Origin Full Year 2017

Top 5 Asia Pacific Countries

1. **China**
2. **South Korea**
3. **Japan**
4. **India**
5. **Hong Kong**

Top 5 Latin American Countries

1. **Brazil**
2. **Mexico**
3. **Argentina**
4. **Colombia**
5. **Chile**

While the C2 breakdown matches closely to the overall malicious traffic by country, it is important to note the person controlling the C2 may not be located in the same country as the C2 server. The location of the C2 is driven by the mechanisms available to the bad actor. The United States is at the top of the list because of the robust networks and volume of devices within its borders. Conversely, countries that allow the unchecked operation of bullet-proof hosting companies will also show a disproportionate volume of C2s within their borders – in this case pushing up Russia and Ukraine higher in the chart. Internet service providers that operate in countries with limited or relaxed regard to laws or regulations governing allowable activity are generally referred to as bullet-proof.

Source: CenturyLink Threat Research Labs, Full Year 2017

CenturyLink®

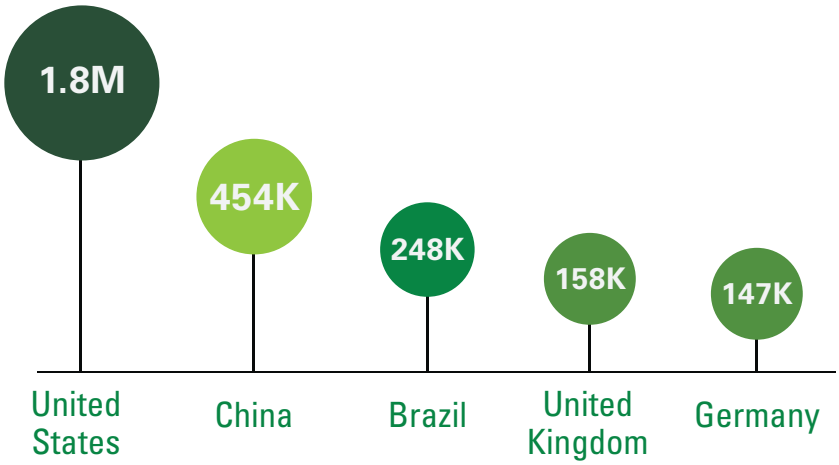
While CenturyLink Threat Research Labs works with providers to take down the supporting services, the bullet-proof hosters seldom comply and, as a result, find their traffic mitigated over our global backbone.

To initiate an effective attack, C2 servers generally need a botnet to control. A botnet is a group of individual compromised hosts, or bots, often controlled by a single C2. A bot can be a compromised server, computer or any IoT device such as a DVR, security camera, cell phone and so on. The most dangerous botnets contain hundreds of thousands of members waiting to attack at a moment's notice – fortunately botnets of this size are becoming rare these days.

As a bot, the compromised device has already been infected by malware. It has communicated with the C2, identifying both what it is and what its capabilities are. Now the bot is just waiting to be directed to launch an attack against a target utilizing a specific set of parameters.

Each of the millions of bots CenturyLink Threat Research Labs tracks was witnessed communicating with a known C2 server.

Top 5 Bot Hosting Countries – Daily Average



Source: CenturyLink Threat Research Labs, Full Year 2017

This chart and the subsequent charts show a more comprehensive view of the bot landscape by region. These hosts have been witnessed interacting with known C2s across the CenturyLink global backbone.

Compromised Hosts (Bots)

by Country of Origin Full Year 2017

Top 10 Countries Globally

1. **United States**
2. **China**
3. **Brazil**
4. **United Kingdom**
5. **Germany**
6. **Canada**
7. **Russia**
8. **France**
9. **Italy**
10. **India**

Top 5 European Countries

1. **United Kingdom**
2. **Germany**
3. **Russia**
4. **France**
5. **Italy**

Source: CenturyLink Threat Research Labs, Full Year 2017

CenturyLink®

Compromised Hosts (Bots)

by Country of Origin Full Year 2017

Top 5 Latin American Countries

1. **Brazil**
2. **Mexico**
3. **Argentina**
4. **Venezuela**
5. **Colombia**

Top 5 Asia Pacific Countries

1. **China**
2. **India**
3. **Japan**
4. **Taiwan**
5. **South Korea**

We've been talking primarily about the bad actors controlling the C2s and the botnets, but it is also important to evaluate the targets of these attacks. Not only are countries and regions with robust communication infrastructure unknowingly supplying bandwidth for these attacks, but they are also the largest targets based on attack command volume.

Source: CenturyLink Threat Research Labs, Full Year 2017

CenturyLink®

Top 20 Countries Globally

Hit with Bot Traffic Full Year 2017

1. United States

2. China

3. Germany

4. Russia

5. United Kingdom

6. Brazil

7. Japan

8. France

9. Italy

10. South Korea

11. Canada

12. Netherlands

13. Spain

14. Taiwan

15. South Africa

16. Sweden

17. Poland

18. Australia

19. Norway

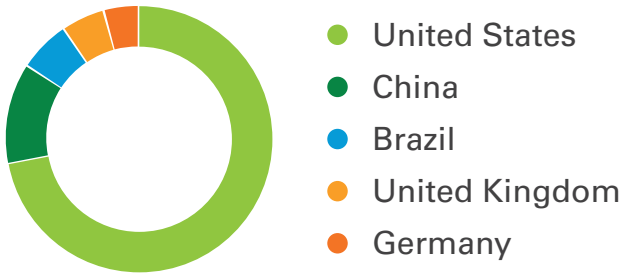
20. Argentina

CenturyLink®

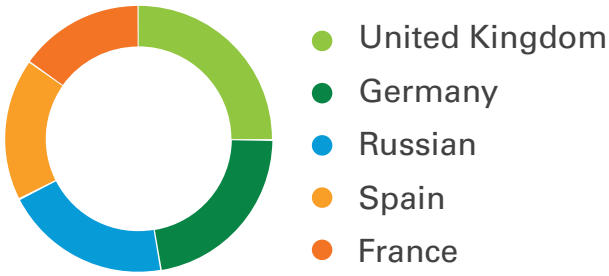
Source: CenturyLink Threat Research Labs, Full Year 2017

In this set of graphs, you can see the distribution of attacks by top target countries and regions.

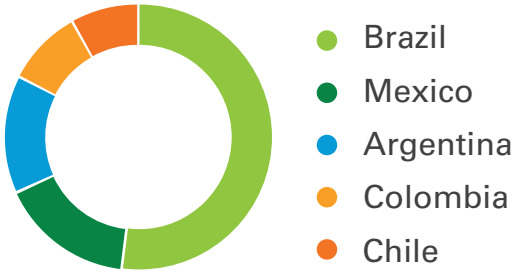
Top 5 Globally
Target Countries Full Year 2017



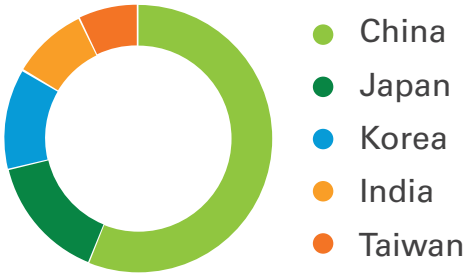
Top 5 European
Target Countries Full Year 2017



Top 5 Latin American
Target Countries Full Year 2017



Top 5 Asia Pacific
Target Countries Full Year 2017



Source: CenturyLink Threat Research Labs, Full Year 2017

CenturyLink®

A Review of DDoS IoT Botnets

Gafgyt and Mirai

The exploitation of IoT devices to create botnets for volumetric DDoS attacks began in earnest within the last several years. As previously reported by the CenturyLink Threat Research Labs, Gafgyt, a precursor to Mirai, started using IoT devices as botnets for DDoS attacks in 2014. Gafgyt (which also goes by the names BASHLITE, Lizkebab and Torlus) is a form of malware architected to infect Linux systems for the purpose of launching DDoS attacks.

Written in C, Gafgyt was designed to be easily cross-compiled for multiple architectures running Linux, making it especially effective in compromising IoT devices and other systems which often use open source operating systems to minimize cost. Gafgyt implements a standard client/server architecture modeled loosely on an internet relay chat (IRC).

Mirai first appeared in the fall of 2016 and quickly proved to be an effective evolution in launching IoT based cyberattacks. Mirai is responsible for launching what was, until March 2018, the largest DDoS attack on record. In addition to attacking krebsonsecurity.com, its variants were responsible for the attack on Dyn, which brought traffic destined for numerous popular websites in Europe and North America to a halt. Since the Mirai source code was released in October 2016, CenturyLink has tracked various evolutions of Mirai, including Satori, Masuta, OMG and Okiru. We continue to work with research peers across the globe to isolate and identify new variants. Because these copycat derivatives are not substantively different to the original Mirai, they are categorized under the header of Mirai in our research.

How IoT botnets work:

Scanning for vulnerable devices is the basis for both botnets. Once vulnerable devices are identified, they are instructed to connect to a download server to install the malware. They then may be instructed to port scan for vulnerable devices or use external scanners to find and harvest new potential bots. In some cases, actors utilize the C2 servers themselves to scan and infect. There is a variety of other infection methods, including brute forcing login credentials on secure shell (SSH) and telnet servers, as well as exploiting known security weaknesses in other services.

How do bad actors decide which malware variant to use? Bad actors have many tools at their disposal when attacking their targets. These DDoS botnets are just a few of the tools they may utilize. We have seen the same operators move back and forth between Gafgyt and Mirai, sometimes attacking the same target.

Mirai and Gafgyt have been tied to DDoS attacks against gaming servers and the botnet owner's perceived rivals. Operators attempt to drive traffic to the gaming servers they control. According to Krebs on Security, a large, successful Minecraft server with more than a thousand players logging on each day can easily earn the server's owners more than $50,000 per month. The revenues come mainly from players renting space on the server to build their Minecraft worlds and purchasing in-game items and special abilities.

They can also operate under a DDoS-for-hire scenario in which they rent their website stressor services to anyone – under the guise that you, as a site owner, want to 'test' or stress your website's connectivity to the internet.

Of course, there is no confirmation that you are the owner of the organization's website that you wish to 'test'.

It is important to note: with both of these families and their operators, targets tend to change frequently. Recently, we have identified several of these operators shifting to bitcoin mining utilizing the bots that they have cultivated to steal their processing resources rather than utilize them in attacks.

C2 count by family – for activity tracked in 2017:

Gafgyt

562 unique C2s tracked in 2017,
minimum uptime - one day,
maximum uptime - 117 days

Mirai

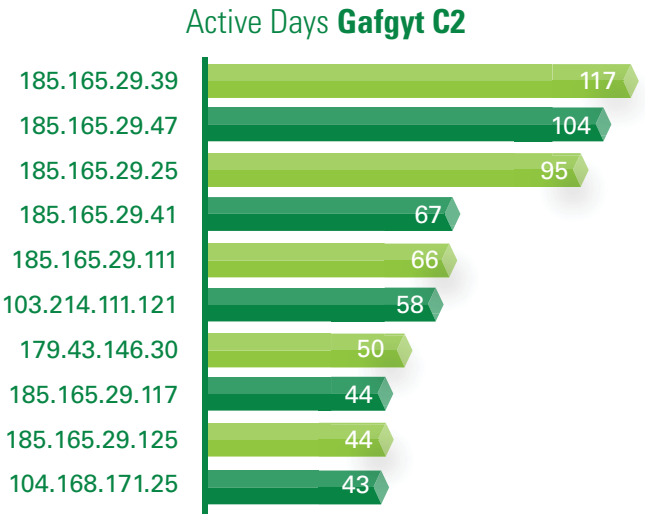
339 unique C2s tracked in 2017,
minimum uptime - one day,
maximum uptime - 83 days

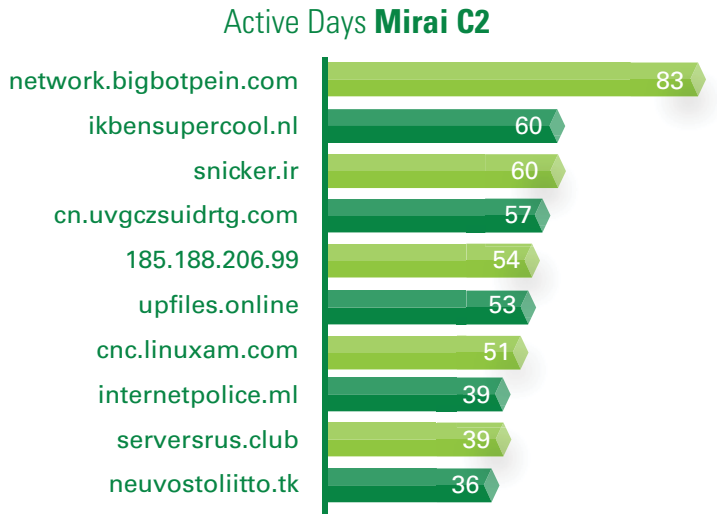
Mirai and its variants have been the focus of numerous headlines and consistent news coverage, but CenturyLink Threat Research Labs has witnessed more Gafgyt attacks affecting more victims, with noticeably longer attack durations.

Top 10 active C2s for each family in 2017:

This chart tracks the top active C2s for the Gafgyt and Mirai botnet families and the length of time they've been active. While CenturyLink cannot fully deactivate a C2 that is not within our sphere of control, we can stop it from accessing our network and resources. However, mitigating a C2 is always a last resort and we aim to work with the broader internet community to resolve the risk first. After a C2 is identified, CenturyLink Threat Research Labs confirms it is a viable threat with intent to harm others and makes several attempts to notify the hosting and upstream service providers of the problem.

Following these attempts, we mitigate the C2's traffic over our global backbone so the cybercriminals cannot use our network resources to perpetrate attacks. In many cases, we even contact the top level domain (TLD) and registrar when required, in an attempt to have the domain deactivated – but this step yields varying results. Therefore, even though the chart below indicates some C2s have been active for up to four months, CenturyLink Threat Research Labs mitigated the traffic within days of identifying the threat, consistent with our desire to be a good steward of the internet.



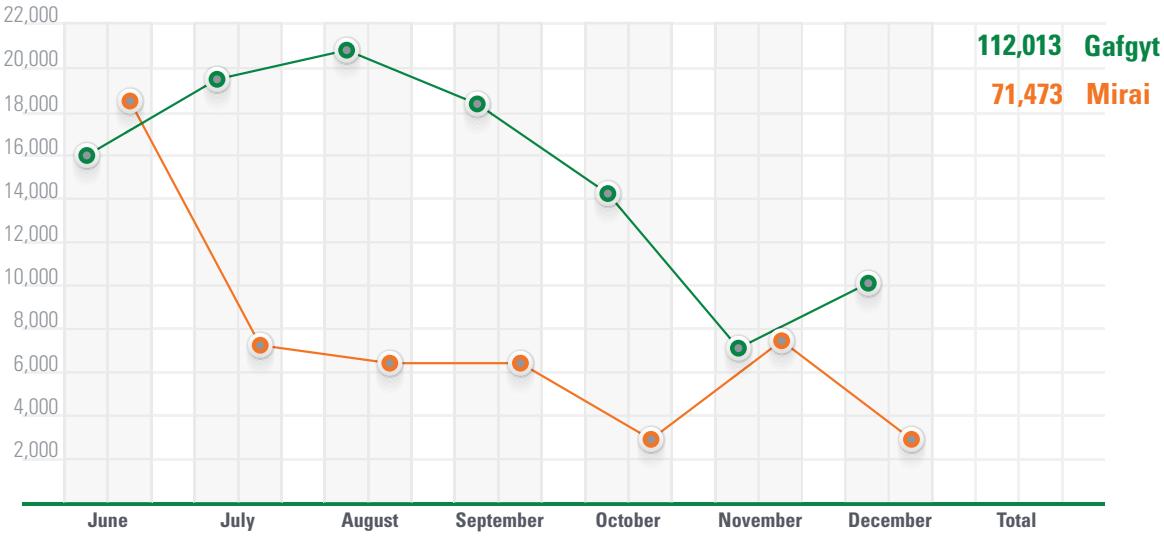


Source: CenturyLink Threat Research Labs, Full Year 2017

The significant maximum uptime for both Gafgyt and Mirai C2s is often a result of bullet-proof hosting providers, as described above.

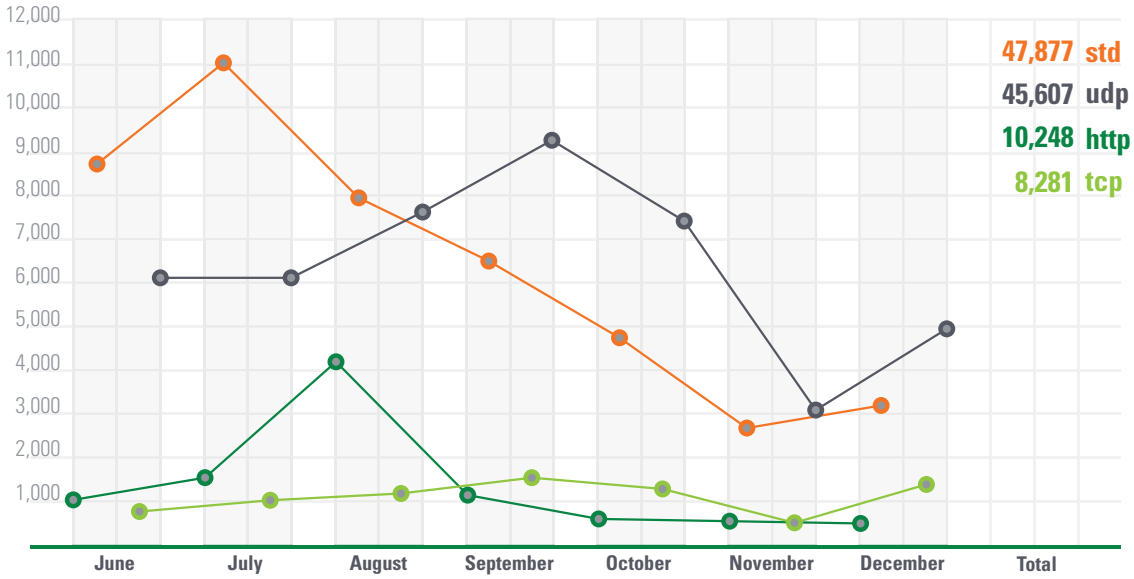
The attraction of Mirai and Gafgyt deployments is that they offer bad actors a wide variety of customizable options to carry out their assaults. The determination of the specific attack type used is based on the capability of the software, the wishes of the malicious client, the target and the desired outcome. Each attack command may include a list of target IP addresses, target domains, ports, services and specified durations.

Attack Commands Issued Total Per Month
2nd Half 2017



The chart below reveals UDP and STD (descriptions below) as the leading attack type for Gafgyt based on our observations.

Types and Volumes of **Gafgyt Attack Commands** Observed
2nd Half 2017

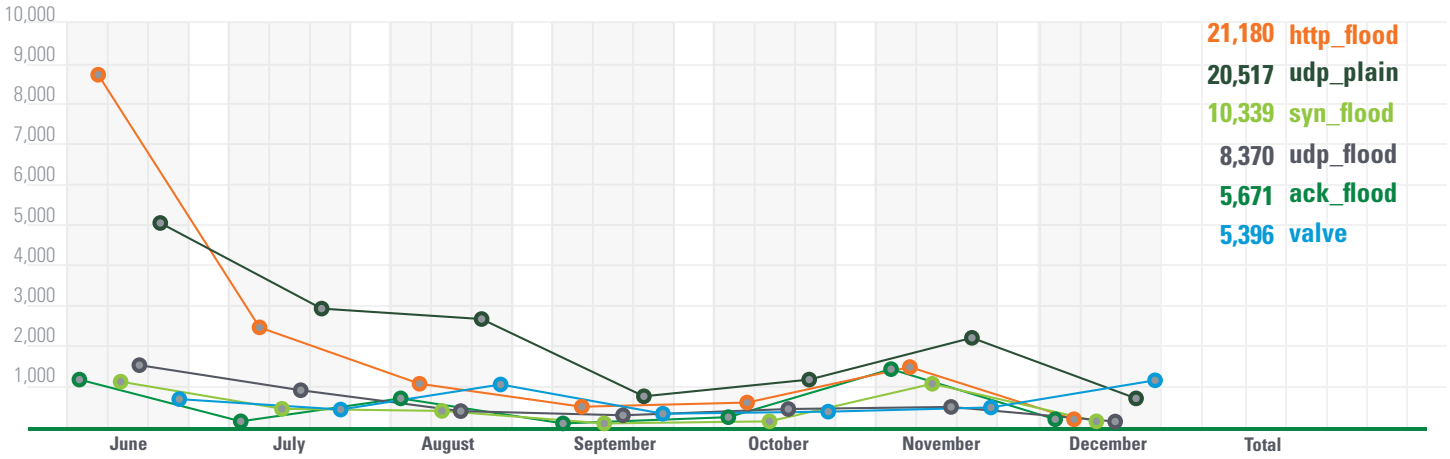


Source: CenturyLink Threat Research Labs, 2nd half 2017

CenturyLink®

HTTP flood and UDP (plain and flood) attacks are the three most commonly used attack types with Mirai, according to our observations.

Types and Volumes of **Mirai Attack Commands** Observed
2nd Half 2017



A Variety of Attack Types Associated with Gafgyt and Mirai

UDP Flood [Mirai] and STD [Gafgyt]
A User Datagram Protocol (UDP) flood attack is used to launch a barrage of packets toward a specific target. In a UDP flood attack, the destination port may be predefined or random. The source port is typically randomized and the source IP can be easily spoofed, protecting the attacker from receiving any responses from the remote targeted system.

Valve [Mirai]
Valve Source Engine Query Flood is a UDP-based attack designed to send Source Engine Query requests, which create excessive resource demands against the target server when sent from multiple spoofed addresses at high volumes. The volume of requests inundates the server, resulting in a denial of service. Bad actors have used this type of attack on gaming servers because of their amplification possibility. When sending this type of query, the server responds back with information about the gaming server and is leveraged to cause game delay or outages for competitive advantage.

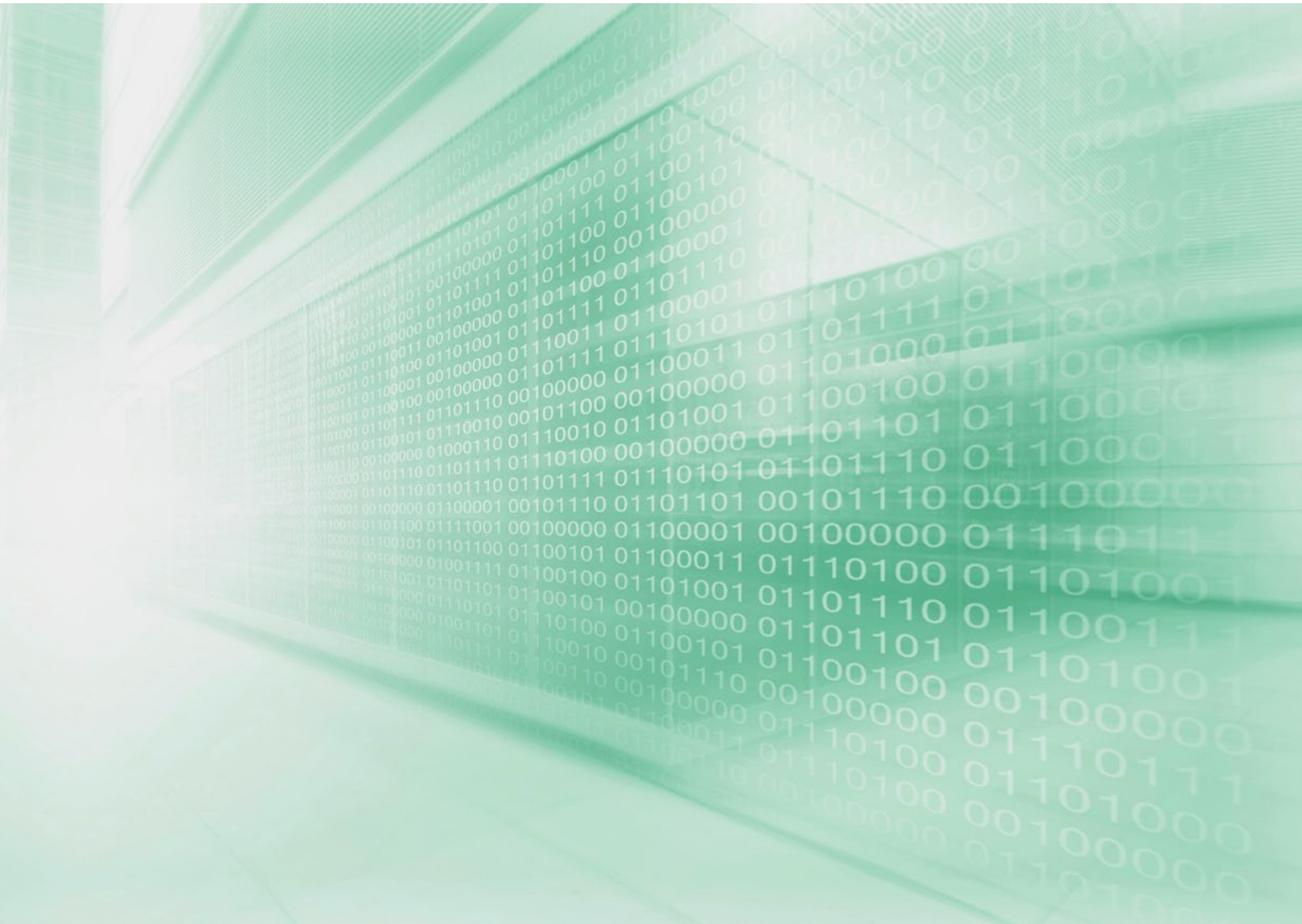
SYN Flood [Mirai] TCP [Gafgyt]
A TCP SYN flood attack involves a bad actor sending successive synchronize (SYN) requests to overwhelm the victim's servers, resulting in its inability to simultaneously respond to legitimate traffic requests.

ACK Flood [Mirai] TCP [Gafgyt]
An acknowledge (ACK) flood attack is closely related to a SYN flood. A bad actor inundates a victim's firewall with spoofed ACK packets in an attempt to overwhelm the server.

Source: CenturyLink Threat Research Labs, 2nd half 2017

UDP Plain [Mirai] UDP [Gafgyt]
The UDP Plain Attack is essentially the UDP Flood attack type, only optimized for speed. Spoofing is not possible with this attack type.

HTTP [Gafgyt] HTTP Flood [Mirai]
The HTTP attack type is instigated as a layer 7 attack. It creates a valid connection with randomized data and HTTP headers are populated based on HTTP response. Assailants can use both GET and POST request types to execute their attack.



Making Sense of the Data

Businesses and government agencies need intelligence that offers the ability to maintain the confidentiality, integrity and availability of data, network resources and other assets.

The CenturyLink Threat Research Labs difference:

CenturyLink Threat Research Labs culls its data from one of the world's largest internet backbones, giving us tremendous depth to our field of vision when it comes to emerging and evolving cyber threats.

CenturyLink collects 114 billion NetFlow records each day, allowing us to capture over 1.3 billion security events daily and to monitor for 5,000 known C2 servers on an ongoing basis.

As one of the leading security research teams in the industry for tracking and reporting on botnets, and due to our unique view of the internet, CenturyLink contributes to several leading media outlets to inform the wider technology community about threats that may impact them, including Ars Technica, CSO, MIT Technology Review, PC Mag, Wall Street Journal, WIRED and many others.

Unlike other security research entities, CenturyLink Threat Research Labs doesn't just passively monitor malicious traffic flowing through the network; the team works to actively prevent bad actors from using CenturyLink network resources to conduct criminal activities. The team identifies dozens of new C2s monthly and works with the upstream service providers to disable their services. If they are unable or unwilling to take action, then CenturyLink steps in and takes measures to protect our network and our customers – nearly 40 C2s per month receive this enhanced treatment.

CenturyLink also collaborates with other leading global threat intelligence teams to share critical insights with the goal of creating a safer internet.

CenturyLink®

To stay abreast of an enemy that is constantly evolving, businesses and governments need to understand the entirety of the threat landscape as it applies to their network. At the same time, threat intelligence without the appropriate filters and customizations can easily result in a flood of information leading ultimately to analysis paralysis.

With the sheer volume and variety of threat types – even within the subset of IoT DDoS attacks – it is easy to lose sight of the most dangerous threats. We see this when news headlines seek to reveal the motives, techniques and sources of threats, yet miss important developments. This is demonstrated by the disproportionate attention paid to Mirai, with its notably shorter dwell time and lower victim count by volume, over that paid to Gafgyt, which has so far shown itself to be a more persistent threat.

As organizations continue to realize operational benefits from greater adoption of cloud-based services, the security perimeter continues to wander and, in some cases, dissolve. Meanwhile, security spend is growing exponentially. By taking a holistic approach to security, one that is informed by actionable threat intelligence, businesses and government agencies can bridge the protection gap.

The scope and depth of CenturyLink Threat Research Labs' intelligence is derived from one of the world's largest IP backbones, critical infrastructure supporting CenturyLink's global operations and those relationships formed with our customers and industry peers. CenturyLink takes a proactive approach to securing the internet: when we see something, we stop it. We believe the internet is a village and each of us must do our part to protect it.

CenturyLink®