2016 DDoS ATTACK TRENDS

NOVEMBER 2016

David Holmes

CONTENT

INTRODUCTION

Remember Huey Lewis and the News? The blues-rock band sounded retro even when they appeared on the scene with their hit, “Hip to Be Square” in 1986. But you know what? It’s 30 years later, and the airwaves are still clogged with their saccharine ballads “The Power of Love” and “I Want a New Drug.”

However, there is a new hit on the airwaves. The Mirai botnet, which harnesses the high CPU capability and high-bandwidth uplinks of hundreds of thousands of Internet of Things (IoT) devices such as DVRs and CCTV cameras has set new records for DDoS attack size, reaching upwards of 1 Tbps. With more and more IoT devices coming online every day (Gartner forecasts that there will be 20.8 billion connected devices worldwide by 2020), the threat of DDoS attacks from increasingly sophisticated IoT botnets will only grow.

While all the focus these days is on this new threat, the old attacks—DNS, NTP, and ICMP fragmentation attacks—are still around, clogging up pipes. They may have lost mindshare and cachet with the media, but they’re still out there, workin’ for a living. And with many easy-to-use DDoS services (often called booters or stressers) managed by the underground, launching effective DDoS attacks is easier and cheaper than ever before.

If you have been watching InfoSec headlines lately, you might be thinking to yourself, “Hmmm, maybe ransomware is the new DDoS?” But just because the cyber-criminal underworld has added ransomware as its latest extortion tool doesn’t mean that they’ve let go of the still lucrative, still too easy, denial-of-service extortion campaigns.

So if the IoT is a new DDoS vector of vulnerability, the old attacks are still around, and ransomware isn’t replacing DDoS, then what does the current landscape of DDoS attacks look like? The DDoS research and defense community is a small one, and they mostly follow each other around between companies. At F5, we have several veterans of the DDoS defense world, and based on their experience, research, and observations fighting DDoS over the last few years, three trends have emerged.

SO, IF THE OLD ATTACKS ARE STILL AROUND, AND RANSOMWARE ISN’T THE NEW DDoS, THEN WHAT IS?

2016 DDoS ATTACK TRENDS

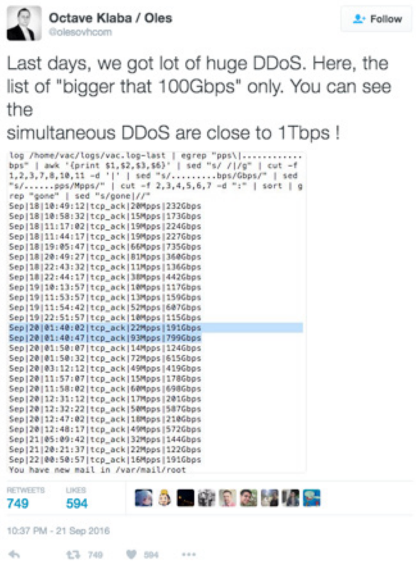
STATEFUL ATTACKS NOW THE MAJORITY

During the DDoS media heyday of 2012–2014, many of the largest and highest-profile DDoS attacks were stateless in that they used protocols based on the User Data Protocol (UDP). Given the unprecedented attacks of 2016, we've had to update our list of favorite stateless attacks:

- The 630 Gbps attack against Krebs on Security
- The 990 Gbps attack against French hosting company OVH
- The 1.2 Tbps attack against DNS provider DYN

UDP is famously easy to spoof: all an attacker needs to do is forge a packet with whatever source address he or she wants. For example, suppose a malicious actor wants to attack your DNS server at 56.26.56.26 with the DNS amplification attack. The attacker creates a set of packets with the source address 56.26.56.26 and then sends them to DNS servers around the world. The DNS servers then respond to 56.26.56.26 (your server), overwhelming it. The same technique works for NTP servers (with the monlist extension), universal plug-n-play devices supporting SSDP, and any ancient server still supporting Chargen, one of the earliest UDP-based protocols.

Stateless protocols have suffered from this weakness for decades, but developing countries are starting to get a handle on it. More and more service providers are implementing "best current practice (BCP) 38." BCP 38 instructs service providers (and other network administrators) to configure their gateway routers to prevent spoofing by dropping outbound packets that have a source address that is obviously not from their network.


Octave Klaba / Oles
@olesovhcom

Last days, we got lot of huge DDoS. Here, the list of "bigger that 100Gbps" only. You can see the
simultaneous DDoS are close to 1Tbps !

```
log /home/vac/logs/vac.log-last | egrep "pps\|............
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ /|/g" | cut -f
1,2,3,7,8,10,11 -d '|' | sed "s/.........bps/Gbps/" | sed
"s/......pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g
rep "gone" | sed "s/gone|//"
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps
Sep|18|19:05:47|tcp_ack|66Mpps|735Gbps
Sep|18|20:49:27|tcp_ack|81Mpps|360Gbps
Sep|18|22:43:32|tcp_ack|11Mpps|136Gbps
Sep|18|22:44:17|tcp_ack|38Mpps|442Gbps
Sep|19|10:13:57|tcp_ack|10Mpps|117Gbps
Sep|19|11:53:57|tcp_ack|13Mpps|159Gbps
Sep|19|11:54:42|tcp_ack|52Mpps|607Gbps
Sep|19|22:51:57|tcp_ack|10Mpps|115Gbps
Sep|20|01:40:02|tcp_ack|22Mpps|191Gbps
Sep|20|01:40:47|tcp_ack|93Mpps|799Gbps
Sep|20|01:50:07|tcp_ack|14Mpps|124Gbps
Sep|20|01:50:32|tcp_ack|72Mpps|615Gbps
Sep|20|03:12:12|tcp_ack|49Mpps|419Gbps
Sep|20|11:57:07|tcp_ack|15Mpps|178Gbps
Sep|20|11:58:02|tcp_ack|60Mpps|698Gbps
Sep|20|12:31:12|tcp_ack|17Mpps|201Gbps
Sep|20|12:32:22|tcp_ack|50Mpps|587Gbps
Sep|20|12:47:02|tcp_ack|18Mpps|210Gbps
Sep|20|12:48:17|tcp_ack|49Mpps|572Gbps
Sep|21|05:09:42|tcp_ack|32Mpps|144Gbps
Sep|21|20:21:37|tcp_ack|22Mpps|122Gbps
Sep|22|00:50:57|tcp_ack|16Mpps|191Gbps
You have new mail in /var/mail/root
```

FIGURE 1. Tweet by OVH chairman Octave Klaba

The adoption of BCP 38 (finally!) is closing the window for spoofed packet attacks like the DNS amplification attack. We can all start pretending that UDP attacks are ending, right?

Wrong.

First of all, developing countries are building out infrastructure faster than they can put controls around it. And they aren't implementing BCP 38 as comprehensively as highly developed, industrialized nations. The F5 Security Operations Center (SOC) is still seeing many 45-minute UDP-based attacks coming from Asia. Operators there, when questioned about BCP 38, give the same response that the more mature operators in the developing countries used to give: “Our network is too big.” That’s just an excuse, of course. It was an excuse then and it’s an excuse now. If you are lucky enough to have a slash 8, then you know exactly what your source addresses should be. Manage it. So even though BCP 38 is good news, the attacks that rely on its absence are still around. They’ve just migrated to where BCP 38 isn’t.

Second, the attackers in the developing countries are getting around the BCP 38 controls by switching to stateful attacks. Stateful protocols, like the TCP, do not, by definition, support stateless attacks like amplification. But there are still plenty of stateful attacks that can be launched over TCP.

For instance, the creator of Mirai talks about the so-called “TCP STOMP” attack, which is a variation of the simple ACK flood intended to bypass mitigation devices. While analyzing the actual implementation of this attack, the bot opens a full TCP connection and then continues flooding the server with ACK packets that have legitimate sequence numbers, in order to hold the connection alive.

ATTACKERS IN THE DEVELOPING COUNTRIES ARE GETTING AROUND THE BCP 38 CONTROLS BY SWITCHING TO STATEFUL ATTACKS

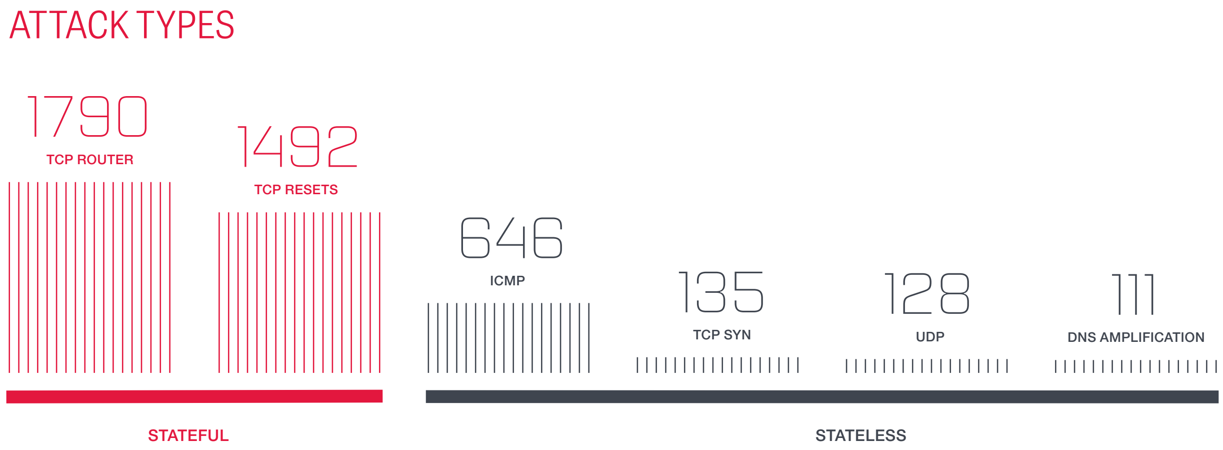


FIGURE 2. Sample of F5 SOC alerts, 2016

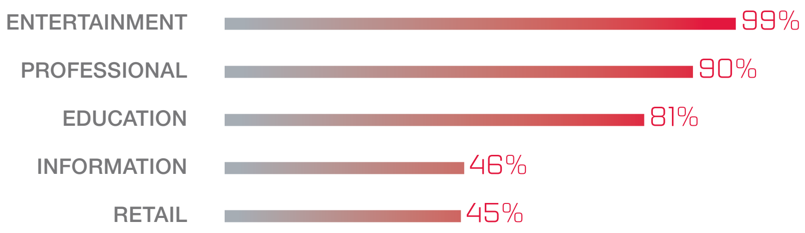
Over the last few years, the F5 SOC has seen TCP-based attacks go from the minority to the majority. Today, in 2016, TCP attacks outnumber UDP attacks by a factor or two to one. This evidence shows that the controls around stateless attacks have pushed the attackers into developing stateful attacks instead.

LAYER 7 ATTACKS ARE THE NEW DRUG

Layer 7 attacks used to be for professional attackers only. The mechanics of a typical layer 7 attack follow a similar pattern: the attacker will find a “heavy” URL on your website (a large PDF file or an expansive database query) and then request it repeatedly—sometimes dozens or hundreds of times a second. When executed correctly, a layer 7 attack can be devastating and very difficult to detect (much less mitigate). Layer 7 attacks aren’t new per se, but they’ve changed in three ways since F5 started quantifying them in 2012.

First, layer 7 attacks are much more common now. Five years ago, we would see them every now and then—perhaps in 10 percent of attack campaigns. Today, the F5 SOC sees hundreds of layer 7 attacks per day. The vaunted Verizon Data Breach Investigations Report (DBIR) (2016 edition) confirms that organizations across all industry verticals are experiencing DDoS attacks.

HIGHEST REPORTED INCIDENTS OF DDoS ATTACKS



.

FIGURE 3. Data from 2016 Verizon Data Breach Investigations Report—security incidents by industry Regulatory compliance. Read full report for additional detail.

First, we’re seeing an evolution in HTTP GET floods, which were already pernicious. Typically, these requests flow right through a standard firewall because they look just like normal HTTP requests to most devices with hardware packet processing. The Mirai attack code takes it a step further by fingerprinting cloud-based DDoS scrubbers and then working around some of their HTTP DDoS mitigation techniques (such as redirection).

We’re also seeing more POST attacks, which malicious actors are using to get around the ubiquity of CDNs like CloudFlare and Akamai. Because HTTP POST commands can change server state, they are usually forwarded directly to the origin servers. Of these, POST attacks against store locators are distressingly common.

Third, where layer 7 attacks used to be very low bandwidth (they were called low and slow for a reason), the F5 SOC is now seeing much larger layer 7 attacks. With proper execution, an attacker sending a custom POST to a store locator over an SSL-encrypted connection can keep a server down with only a tens of thousands of bits per second. But today we are seeing regular layer 7 attack campaigns of 300 Mbs. That's a huge amount of layer 7, if the attack is crafted to leverage asymmetrical properties. The F5 SOC is also recording more layer 7 attacks of 8–10 Gbs, which we rarely saw three years ago.

The final change in layer 7 DDoS attacks involves the evolution of communications between botnet participants and their command-and-control (C2) servers. C2 servers relay attack commands to botnet hosts and are therefore the critical infrastructure component for botnets. As such, C2 servers are prime targets for take-down services (such as Microsoft, CERT, F5, among others). Over the years that F5 has been running take-downs, attackers have evolved some fascinating new techniques for hiding C2 communications.

We're seeing more peer-to-peer and multi-tier communications networks within botnets, as attackers work to hide their command channels. An excellent example of the latter architecture is documented in the RUAG cyber-espionage case in Switzerland, where the (unknown) attackers used several layers of proxies both within and without the victim network to mask the ultimate location of the C2 server.

More recently, the Mirai malware C2 infrastructure has compromised and communicated with hundreds of thousands of IoT devices since the source code was made public in October. The malware scans the Internet in search of connected and vulnerable devices (those with default or weak passwords), which it then recruits to join an ever-growing botnet. In order to defeat attempts at detection and dissolution, only a few C2 IP addresses are active at any one time, with new ones coming online every few days.

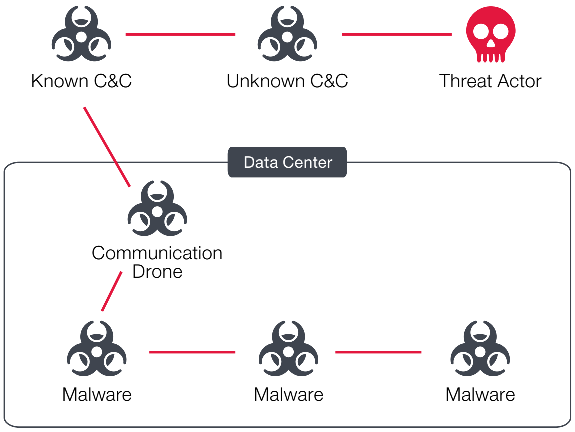


FIGURE 4. Sophisticated C2 architecture seen in RUAG CyberEspionage APT

An even more exotic, almost boutique, C2 communications system was discovered in a botnet where the botnet participants would receive coded instructions hidden inside Twitter avatar images (an information-hiding technique known as steganography).

DNS ATTACKS STILL BEATIN’

In 2013, the so-called Spamhaus attack set the record for the (at the time) largest DDoS attack campaign of all time at over 300 Gbs. The Spamhaus attack campaign leveraged millions of misconfigured open DNS resolvers around the world for DNS amplification attacks. The Open Resolver project was started in response to the attack. The project was tracking 22 million open resolvers in 2013, but after a year the number had not shrunk. In fact, it had grown to 32 million.

Many millions of these open resolvers are still out there, meaning that it is still a free, high-powered botnet available to anyone with the knowhow to leverage it. In spite of the project, and the awareness campaigns, the heart of DNS amplification is still beating. And we at the F5 SOC are still seeing the same number of DNS attacks, but with many more different types of attacks available, the “market share” share of DNS attacks has decreased.

However, as is shown by the devastating Dyn attacks, DNS remains a vector of vulnerability. A significant percentage of DNS services are still under-provisioned to the point where they are unable to withstand even small-to-medium-size DDoS attacks. DNS caches have become popular as they can boost the perceived performance of a DNS service and provide some resilience against standard DNS query attacks.

As DNS defenses have evolved, so have the methods used by attackers. Attackers have switched to what is called “no such domain” (or NXDOMAIN) attacks, which quickly drain the performance benefits provided by the cache. In addition, the Mirai malware enables attackers to launch a “water torture” attack against a target DNS server. This technique is different from the regular DNS reflection and amplification attacks as it requires significantly fewer queries to be sent by the bot, letting the ISP’s recursive DNS server perform the attack on the target’s authoritative DNS server.

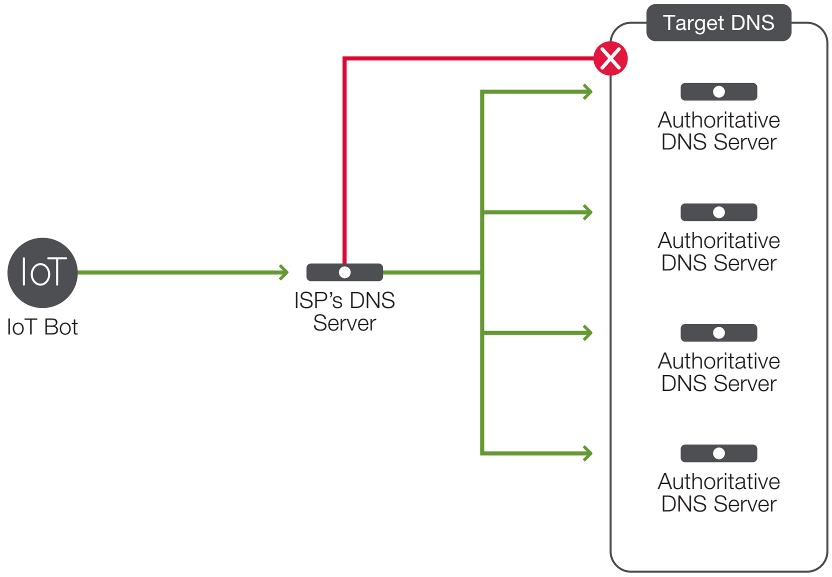


FIGURE 5. DNS water torture attack

In this attack, the bot sends a well-formed DNS query containing the target domain name to resolve, while appending a randomly generated prefix to the name. The attack is effective when the target DNS server becomes overloaded and fails to respond. The ISP's DNS servers then automatically retransmit the query to try another authoritative DNS server of the target organization, thus attacking those servers on behalf of the bot. In their post-mortem on the October 21 attacks, Dyn confirmed that this DNS water torture attack was used successfully to increase traffic volume and negatively impact the DNS provider's network.

IN CONCLUSION: IF THIS IS IT, WHAT CAN BE DONE?

The Mirai attacks prove that DDoS attacks are not only going away, but are entering a new phase. However, one of the reasons DDoS attacks keep evolving is that defenders keep evolving as well, so understanding these latest trends can help you be better prepared. With the emergence of new big-and-smart attacks, layer 7 mitigation is critical. There are more stateful attacks; low and slow has become big and smart (100 Gbs layer 7 POSTs are the new norm); and on top of it all, organizations must still defend against old attack methods.

The most resilient architecture to help combat these attacks is a combination of on-premises and cloud DDoS scrubbing to mitigate network, application, and volumetric attacks. As we mentioned, the adoption of BCP 38 is making a difference. Yes, it's driving attackers to the less developed world or forcing them to evolve to layer 7 attacks, but that doesn't mean BCP is an invalid idea. Preventing spoofing on a large scale should be a goal of the Internet. And finally, regulation will likely be the best fix for the IoT vulnerabilities that led to the successful Mirai botnet attacks. Consumer devices are already regulated for safety and efficiency; it's time they're also evaluated for Internet security.

But, at the end of the day, those that maintain their vigilance with investments in both on-premises and cloud DDoS-scrubbing partners will be best prepared to navigate the ever-changing DDoS-risk landscape.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan K.K.
f5j-info@f5.com

Solutions for
an application world.