NEXUSGUARD®
Global Leader in DDoS Mitigation

Threat Report

DDoS Threat Report
Reflection Attacks

Q3 2016

456 Montgomery Street, Suite 800 San Francisco, CA 94104 USA | +1 415 299 8550

nexusguard.com
sales@nexusguard.com

Methodology

As the global leader in Distributed Denial of Service (DDoS) mitigation, Nexusguard observes and collects real-time data on threats facing enterprise and service-provider networks worldwide. The data contained in this report is sourced from our external hybrid Darknet, which is run and maintained by Nexusguard and its associated community of leading anti-DDoS and Internet-cleansing organizations.

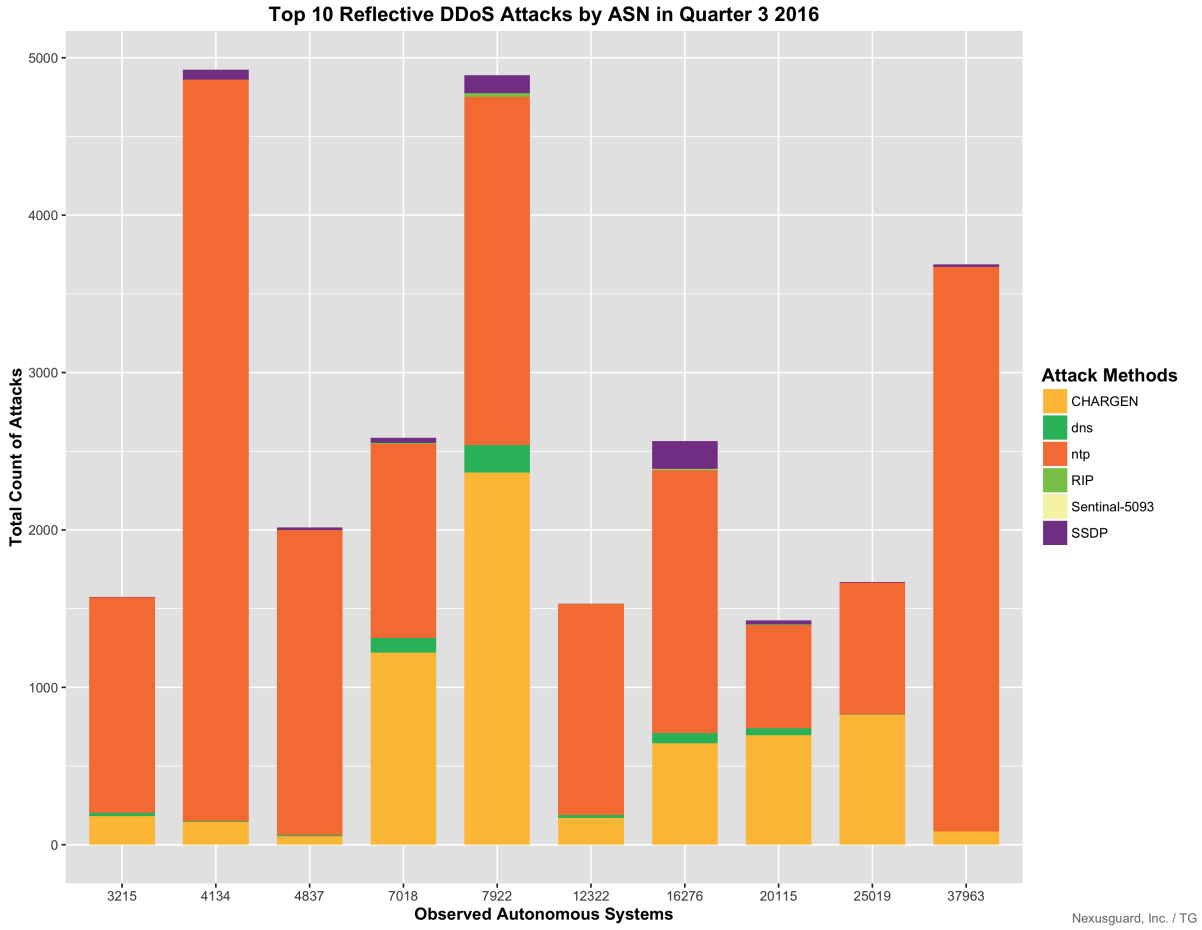
A network of vulnerable, Internet-connected devices and honeypots comprises Nexusguard's collaborative Darknet, uniquely positioning it to measure global events in a manner that is not biased by any single set of customers or industries. Many zero-day threats are first seen on Nexusguard's global research network. These threats are summarized in our quarterly reports.

Introduction

In Q3 2016, reflection-based DDoS attacks decreased, while botnets picked up more headlines. The quarter did, however, see a few notable DDoS attacks that made international news: one targeting Brian Krebs, a journalist covering the cybercrime beat, and another hitting OVH, an Internet hosting provider. Both attacks utilized botnets, which isn't rare, although the speeds with which they were launched were unprecedented for botnets. A branch of the jgamblins github containing the source code can be seen here: https://github.com/kingtuna/Mirai-Source-Code. The botnet (Mirai) consisted of systems that were on-boarded via telnet password cracking in a process that the coder described as a real-time load. It's interesting that the botnet used GOLang to control the environment (we switched over C for our service emulation).

Overall, the quarter was characterized by a daily downtick in the average number (1269) of reflection-based DDoS attacks, a decrease on nearly 40%.

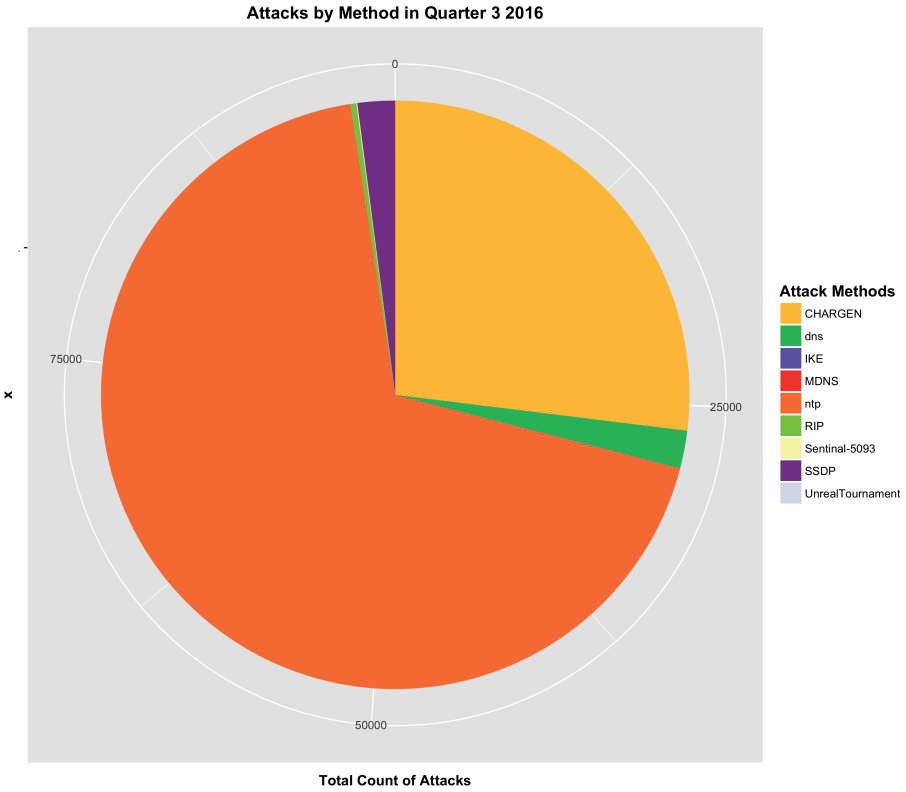
Top 10 Reflective DDoS Attacks by ASN in Quarter 3 2016



Regarding network rankings: With 7034 attacks, Starlink was the top targeted network last quarter. In Q3, however, Starlink dropped off the Top 50 list of attack destinations, increasing our suspicions that it was merely an outlier last quarter. In Q3, AS 4134 was the top target destination, and it was obviously not an outlier as it has consistently shown up in our Top 10. Echoing the overall decrease in attacks this quarter, it's no surprise that our top targeted network decreased by 40% — the same decrease we saw in attacks-per-day.

AS	Count	Network Name
4134	4925	CHINANET-BACKBONE No.31, Jin-rong St., CN
7922	4889	COMCAST-7922 - Comcast Cable Communications, Inc., US
37963	3687	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Adv. Co., Ltd., CN
7018	2586	ATT-INTERNET4 - AT&T Services, Inc., US
16276	2564	OVH OVH SAS, FR
4837	2016	CHINA169-BACKBONE CNCGROUP China169 Backbone, CN
25019	1669	SAUDINETSTC-AS Saudi Telecom Company JSC, SA
3215	1574	AS3215 Orange S.A., FR
12322	1530	PROXAD Free SAS, FR
20115	1426	CHARTER-NET-HKY-NC - Charter Communications, US

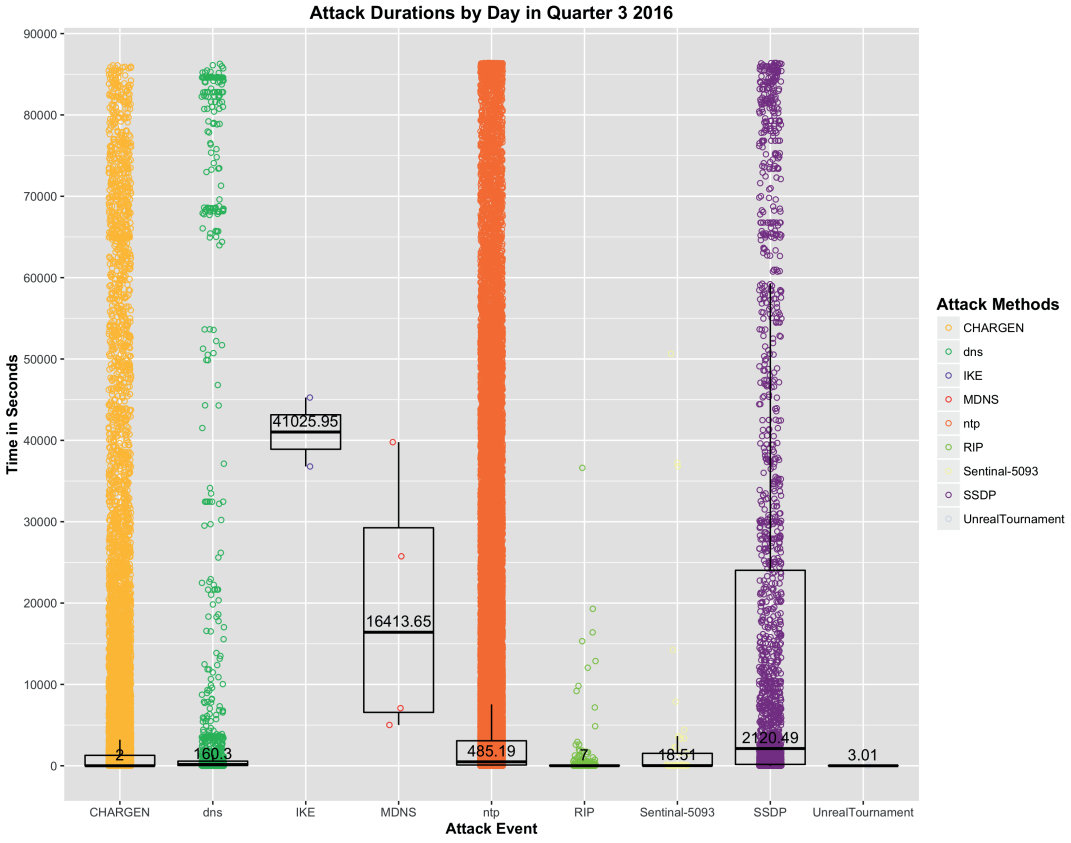
Attacks by Method in Quarter 3 2016



Regarding attack methodology: In keeping with fewer attacks overall in Q3, DNS-based reflection attacks also saw a major dip in the quarter. Last quarter we observed that DNS was creeping up on NTP as the primary method of attack. But now, DNS has all but completely disappeared with a decrease of 97%. This number alone can account for the 40% drop in attacks. While NTP attacks were down by 21%, the ratio was up to about 66% of the total, making NTP the reflection attack method of choice. Additionally, CHARGEN increased 109%. But the CHARGEN attacks were well distributed, so an outlier was most assuredly behind the increase: Note that the main target for the CHARGEN attacks was a residential customer on the Time Warner Cable Network.

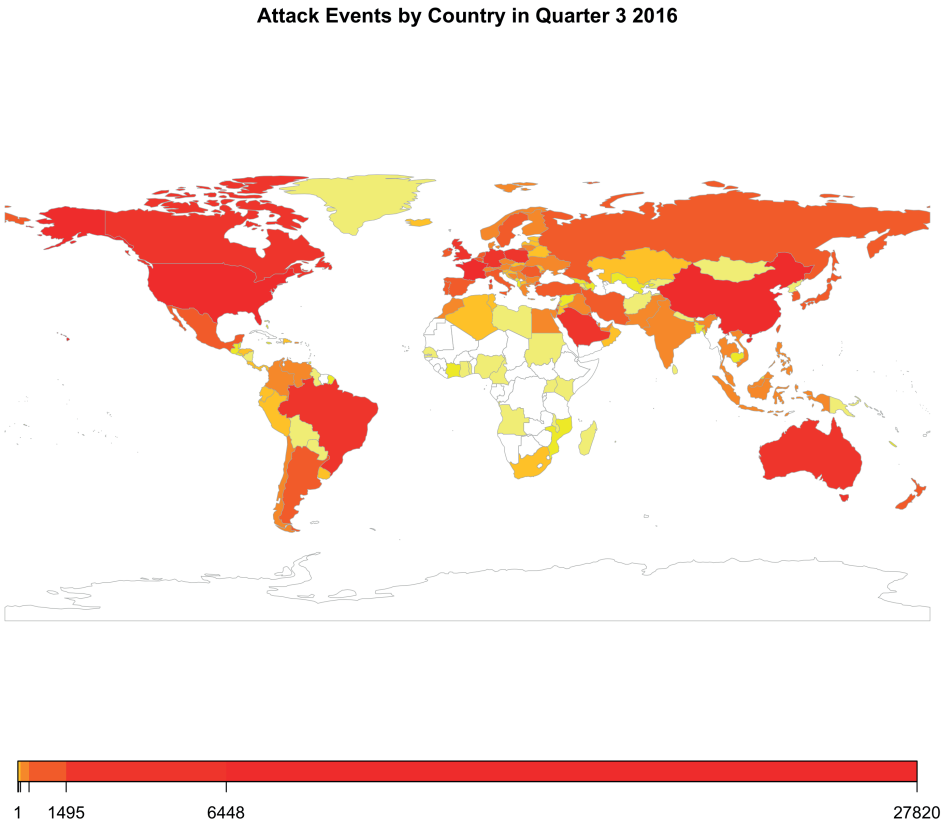
Rank	Method	Count
1	NTP	66975
2	CHARGEN	26337
3	DNS	2027
4	SSDP	2014
5	RIP	320
6	Sentinal-5093	52
7	MDNS	4
8	IKE	2
9	UnrealTournament	1

Attack Duration by Days in Quarter 3 2016



Regarding attack duration: Wow! Two- and three-second attacks. What could this possibly mean? 1) Perhaps the lists the attackers are using are getting larger and thus prompting fewer requests — but they would have to be pretty large, and we consider it unlikely with servers reaching 150K packets per second; 2) Maybe the attackers servers were overwhelmed and unable to send out traffic fast enough; 3) The attacks were just shorter for no reason in particular. In the quarter, NTP attacks regularly jumped over the 300-second mark, while SSDP attack lengths stayed about the same

Attack Events by Country in Quarter 3 2016



Regarding attack events: Last quarter we talked about the Big Three: Russia, China, and the US. This quarter, we have other countries that consistently make the Top 10, but rarely get as much attention. To wit: At Number Three, France was home to the largest recorded DDoS attack this quarter coming in at 1Gbps. The "winner" of such a large attack was the hosting service provider OVH, which unsurprisingly received the highest numbers of attacks in France and also had the top target. The only reason we suspect that OVH didn't reach the Tbps mark is that many of the DDoS attacks were actually internally sourced from OVH. At any rate, this is only speculation and there is no evidence to prove the accuracy of the numbers.

Conclusion

In closing: Last quarter France was Number Four, but it bumped up to Number Three in Q3. The US is now Numero Uno with a 16% increase in attacks, while China has seen a drop of 33%. The big loser (really winner) was Russia dropping from Number One in Q2 down to the twelfth spot with only 2% of the attacks in Q3 2016.

Country	Count
US	27838
CN	19024
FR	7194
GB	4925
SA	3547
CA	3062
DE	2956
AU	2570
HK	2499
PL	2150

NEXUSGUARD®

Global Leader in DDoS Mitigation

All data used to generate this attack report as well as the project used to monitor the honeypots will be published to https://github.com/kingtuna/Hybrid-Darknet-Concept

456 Montgomery Street, Suite 800 San Francisco, CA 94104 USA | +1 415 299 8550

nexusguard.com
sales@nexusguard.com