NEXUSGUARD®

Threat Report

Distributed Denial-of-Service (DDoS)

Q1 2016

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.

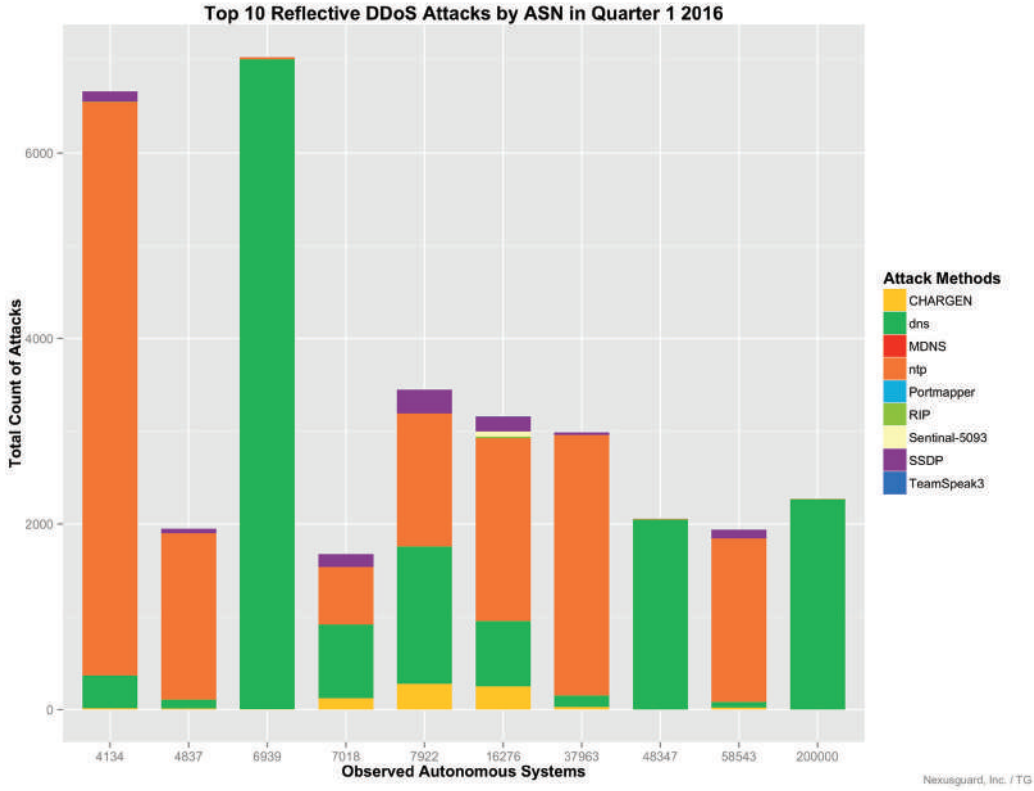
A network of vulnerable, Internet-connected devices, or honeypots, comprises Nexusguard's collaborative darknet, uniquely positioning it to measure global events in a manner that is not biased by any single set of customers or industries. Many zero-day threats are first seen on Nexusguard's global research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

Introduction

Q1 2016 has been incredibly interesting. New reflection services have been discovered, companies have increasingly become targets, and unexpectedly, the Number One target for DDoS attacks was DDoS researchers themselves. When analyzing our honeypot data, it came as no surprise that the majority of Internet- based scans was being conducted by research companies. But what was surprising is that the highest volume of attacks targeted researchers at Loryka LLC, which received 90 attacks in the quarter.

Currently protected by a DDoS mitigation company, Loryka was hit nearly every day, with NTP being the service of choice for the infrastructure attacks. We reached out to Justin Shattuck of Loryka who confirmed that the attacks targeted his research page (he noted that the page was just a landing page that contained no actual research data).

Top 10 Reflective DDoS Attacks by ASN in Quarter 1

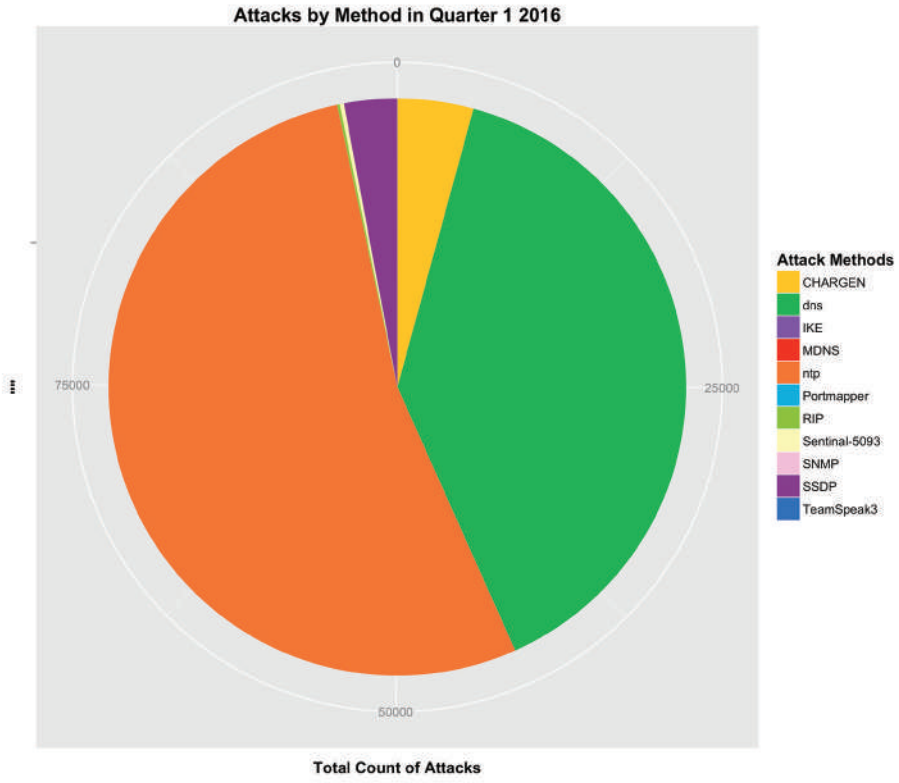


As far as ASN targets go, it's interesting to note that Turkcell and Turkish Telecom are no longer in the Top 10. This adds further confirmation that Turkey's Q4 2015 high ranking was a fluke, as we hypothesized that attacks targeting Turkish entities in the quarter had much to do with Turkey's downing of a Russian fighter jet.

In Q1 2016, we saw a new comer to the Top 10: Hurricane Electric. The majority of attacks targeting the company came during the UTC days of 2016-03-01 and 2016-03-02. As seen on the chart above, DNS comprised the majority of the attacks. This is interesting because most of the DNS ANY requests used the query "freeinfosys.com," an older amplification domain that has had its record greatly reduced in size.

AS	Rank	Fullname	Count
6939	1	HURRICANE - Hurricane Electric, Inc., US	68296
4134	2	CHINANET-BACKBONE No.31, Jin-rong Street, CN	42522
7922	3	COMCAST-7922 - Comcast Cable Communications, Inc., US	5910
16276	4	OVH OVH SAS, FR	4361
37963	5	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co., Ltd., CN	4150
200000	6	UKRAINE-AS Hosting Ukraine LTD, UA	4064
48347	7	MTW-AS JSC MediaSoft Ekspert, RU	3206
4837	8	CHINA169-BACKBONE CNCGROUP China169 Backbone, CN	3144
58543	9	CHINATELECOM-GUANGDONG-IDC Guangdong, CN	2837
7018	10	ATT-INTERNET4 - AT&T Services, Inc., US	2350

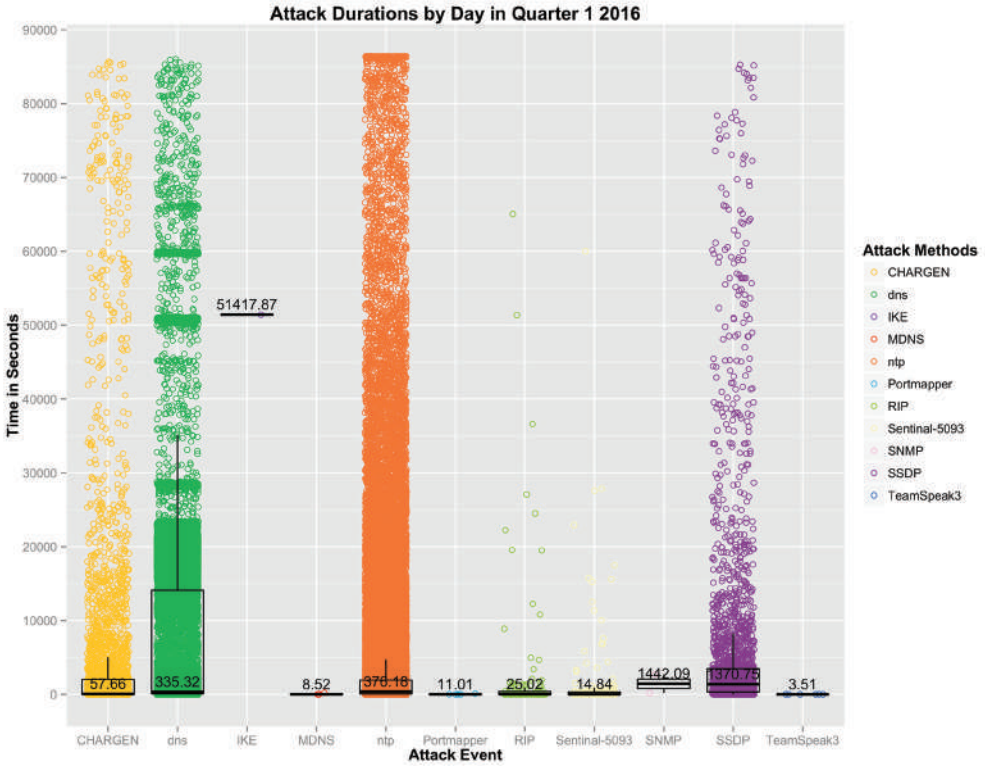
Attacks by Method in Quarter 1 2016



Other interesting developments: We saw our first IKE and MDNS attacks in Q1 2016. Looking at the diversity of attacks, it's noteworthy that last quarter's attacks targeting Turkey skewed the number of NTP attacks, and now again in the first quarter of this year, NTP was the preferred method of reflective DDoS. While we expect to see the increased diversity of attacks continuing, we also predict that attackers will stay true to their classic methods.

Rank	Method	Count
1	NTP	53263
2	DNS	39006
3	CHARGEN	4243
4	SSDP	2957
5	Sentinal-5093	228
6	RIP	144
7	TeamSpeak3	6
8	Portmapper	5
9	MDNS	4
10	SNMP	2
11	IKE	1

Attack Duration by Days in Quarter 1 2016

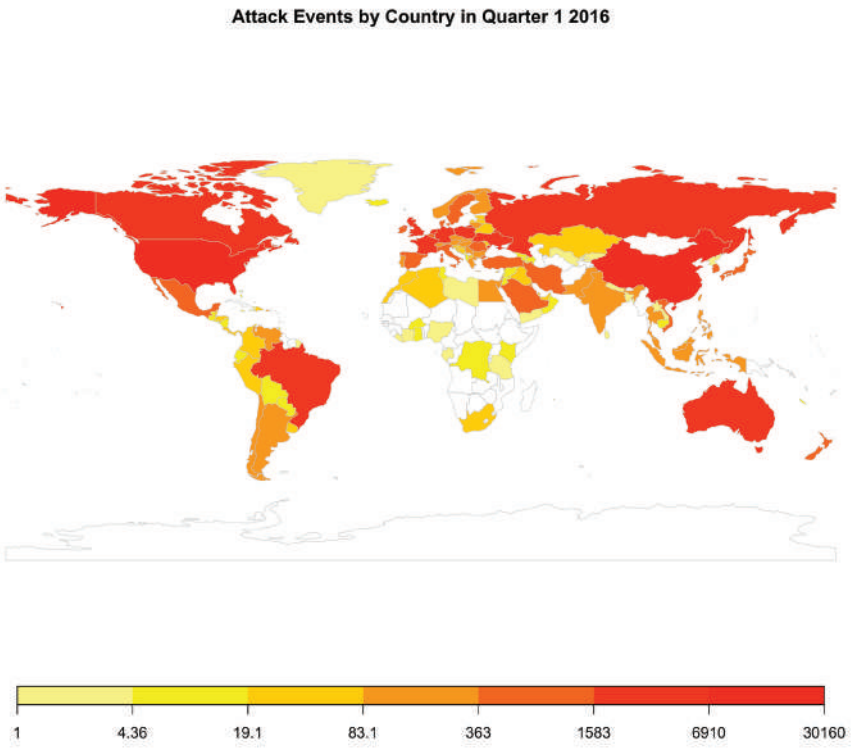


Attack durations are monitored by day and visualized in seconds. This is done because the data is analyzed daily and attack tools are generally executed with a second-based timer. This can be seen in the medians around the durations.

With the large sample sets we gathered in Q1 2016, we saw a pattern of 300-second attacks coming very close to representing the mean. We hypothesize this to be the result of attacks generated by DDoS for-hire sites. It is much more apparent in DNS, where you can see the lines created around standard attack lengths. This appears to be the case quarter after quarter, except for IKE — the only attack that had an extremely long duration. That's because, in instances as described by a fellow researcher, the response to the request lasted indefinitely.

Overall, most attacks last less than ten minutes, with the mean close to five. So in order to have effective detection for these short-lived events, monitoring needs to be on a second- or sub-second-based interval, which generally obviates the use of standard netflow detection methods.

Attack Events by Country in Quarter 1 2016



With Turkey out of the Top 10, it's now time to redirect our attention to the old standbys. Not surprisingly, the US and China bore the brunt of attacks observed in the quarter. We predict the same distribution next quarter, provided that there are no geopolitical conflicts impacting DDoS-prone countries. Going beyond the Top 10 attack targets, we see an increasing focus on the Middle East, and will keep a close eye on the region in future reports.

Rank	Country	Count
1	US	30155
2	CN	18857
3	BR	5823
4	GB	4510
5	FR	4081
6	DE	3756
7	RU	3654
8	CA	2829
9	UA	2564
10	PL	2536

Conclusion

Over the past few years there has been an evolution in the roles of prey and predator, where the game of cat and mouse has become one of seal vs. the great white shark. No longer are digital enthusiasts breaking into networks to brag to their friends about their capabilities. Instead, they are launching full-scale digital operations and absconding with terabytes of data that are affecting some of the world's largest corporations. Some of these operations are government sponsored, where official agencies are utilizing hackers as clandestine guerrilla warfare groups. And clearly, it is very sophisticated warfare, where the Number One target — as we've seen this quarter — includes scientists and researchers. Now, no one is safe from attacks.

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