QRATOR

wallarm

Network Security in 2016

Main events, trends and details

February 2017

Qrator and Wallarm 2016 State of Network Security report is dedicated to the main events and strong trends in the network security industry.

Particular attention is payed to the DDoS, Internet infrastructure, hacks and vulnerabilities in software and hardware, like connected devices.

For eight years Qrator and Wallarm explore attacks on and hacks of the various parts of the Internet.

This report is based on:

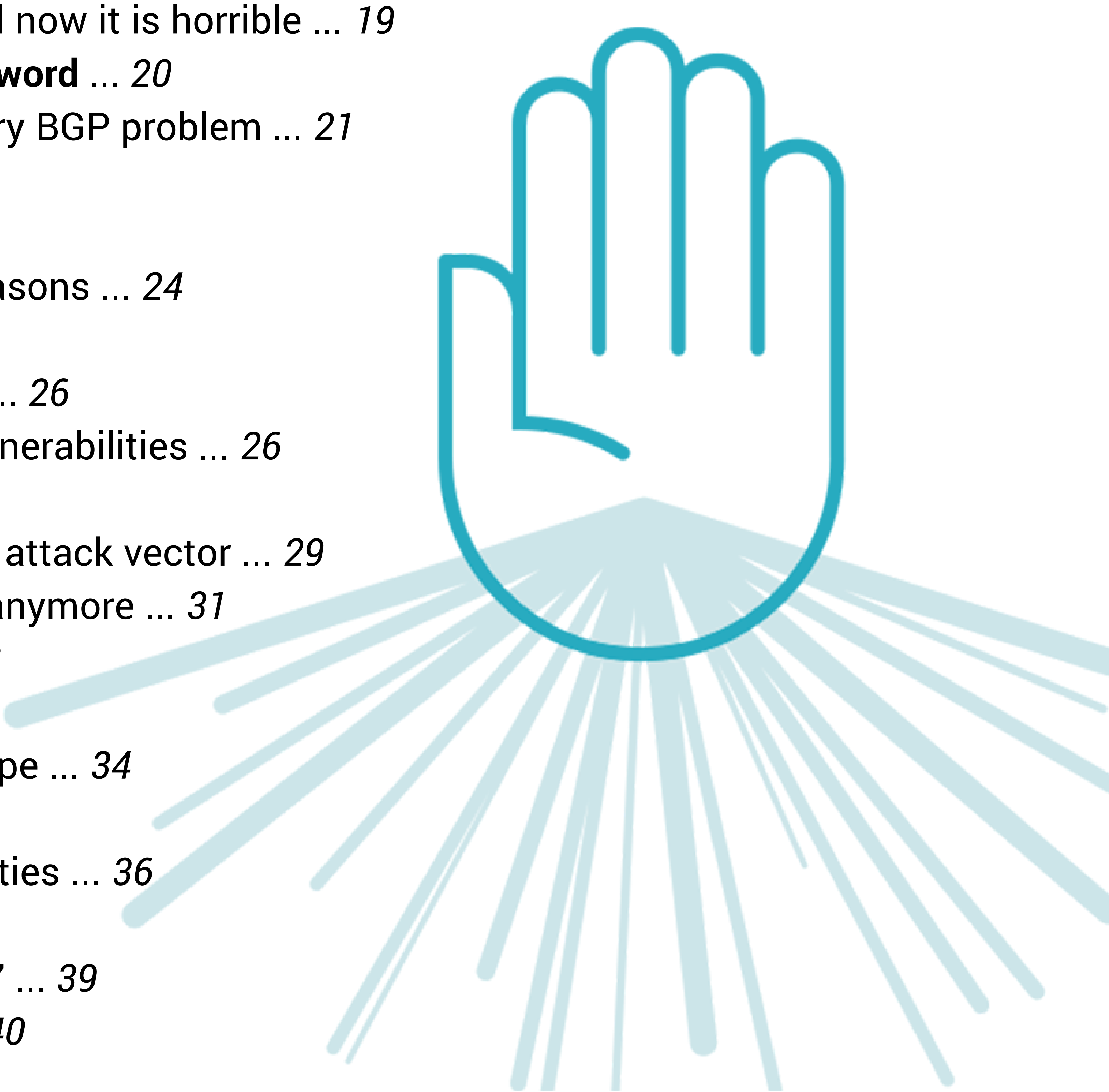
1. **Companies expert observations**, and technical support data, attacks mitigated and vulnerabilities patched.

2. **Worldwide communication** with experts within technical meetings, conferences, and organizations like IETF.

3. **Qrator Radar data** — global autonomous system (AS) interconnection, and incidents monitoring tool.

4. **Wallarm data** — traffic analysis, breaches, vulnerabilities, and hacks information.

Table of Contents



1. Introduction

2016 was the year of a paradigm shift in a network security landscape

Qrator Labs and Wallarm made three predictions at the end of 2015 which were fully realized during 2016

Simplification of hacks and attacks down to the tutorial and how-to level of entry

We saw a dramatic drop in the required level of expertise and knowledge needed to become a malefactor. Nowadays, a simple how-to video on YouTube or a Bitcoin-prepaid stresser/booter is enough to perform an attack successful against even larger websites and applications — something unseen in previous years.

Hacks and malware infections of the IoT and infrastructure, DDoS attacks using botnets of these hacked devices

Brian Krebs is now probably the most demanded cyber security expert in the field: he was among first to tell about the evolution of Mirai and cover some of the security breaches and vulnerabilities. For his many years of hard work as a security journalist, his investigations of computer hacks and paths people take to become cybercriminals he was chosen as a target. Akamai which hosted Krebs's blog on pro bono basis could not withstand a record-setting 620 Gbps attack by Mirai botnet and shut him off. However, as Brian says, censorship would not work over the internet, as he continues to investigate malicious and criminal activity over the web.

Infrastructure vulnerability, high collateral damage attacks

Late 2016 we witnessed the first, but not last, IoT-based botnet — Mirai. Hundreds of thousands of routers, cameras, DVRs, and other connected devices, even Wi-Fi-enabled coffee-makers, made one the biggest media stories of the year in the professional security community, hunting down Dyn, one of the world's largest DNS providers. A fast and merciless attack made the world's most visited websites unavailable for hours, showing extreme collateral damage in a thoughtful infrastructure attack. Before that Mirai raised the bar of a possible threat by performing a 1 Tbps attack on OVH, a French cloud hosting provider, one of the biggest in its class.

Much more than just three attacks

Three events listed above represent not even the half of what's happened last year, but they mark the significant shift in the DDoS and, in general, network attacks that have been predicted, overseen and recorded by Qrator Labs & Wallarm.

Brian Krebs, OVH, and Dyn attacks mark a new era in DDoS. At the same time, they sign arrival of the age of the Internet of Things. Its current device count is probably somewhere between Gartner's estimate of 6,5 billion (excluding computers, tablets, and smartphones), International Data Corporation's 9 billion (again, without those mentioned), and IHS's reckoning of 17,6 billion devices connected, everything inclusive. The consensus is that in 2020 there would be from 20 to 30 billion devices connected to the Internet.

And not just quantity of attack rises — the quality too. DNS defenses have evolved, so have the methods, vectors, and tools, used by attackers. So-called ”no such domain” (NXDOMAIN) attacks showed their effectiveness by quickly draining performance out of the cache. Mirai used a “water torture” technique against its target DNS servers. It is different from regular DNS reflection and amplification attacks and allows recursive DNS server perform the attack on the target's authoritative DNS server.

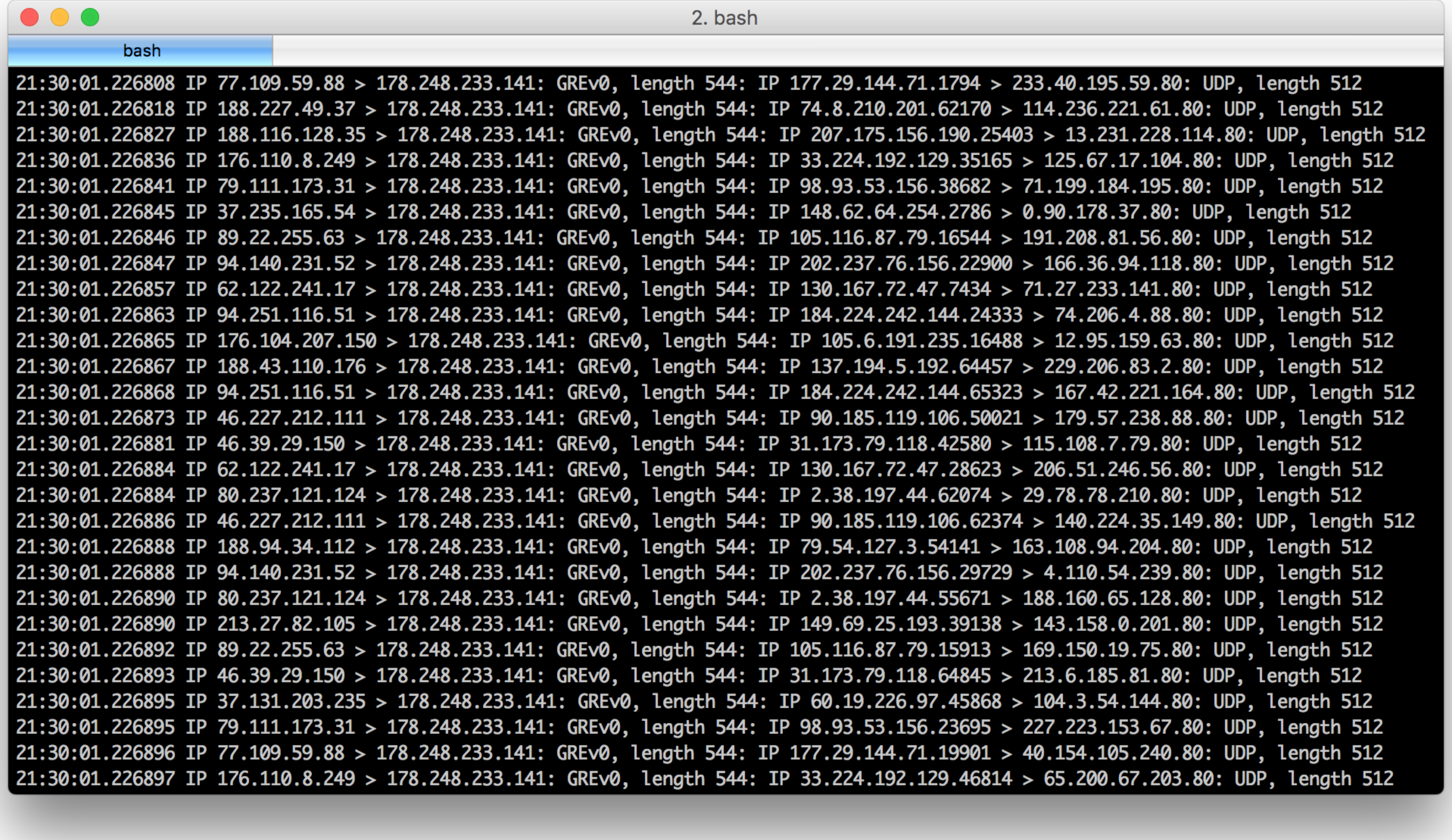
As a mitigation service provider, we see an ongoing evolution of attacking tools, techniques, and networks. In this document, we report what we see as dangerous, possible and evident in the current state of network security, DDoS, infrastructure and developer operations security.

"Qrator did encounter Mirai botnet in form of a 120 Gbps attack. An attack was neutralized, and no clients suffered any downtime issues."

Next: 2016 Highlights

2. Highlights of the year 2016

3 DDoS world records in one month:
from Brian Krebs to Dyn



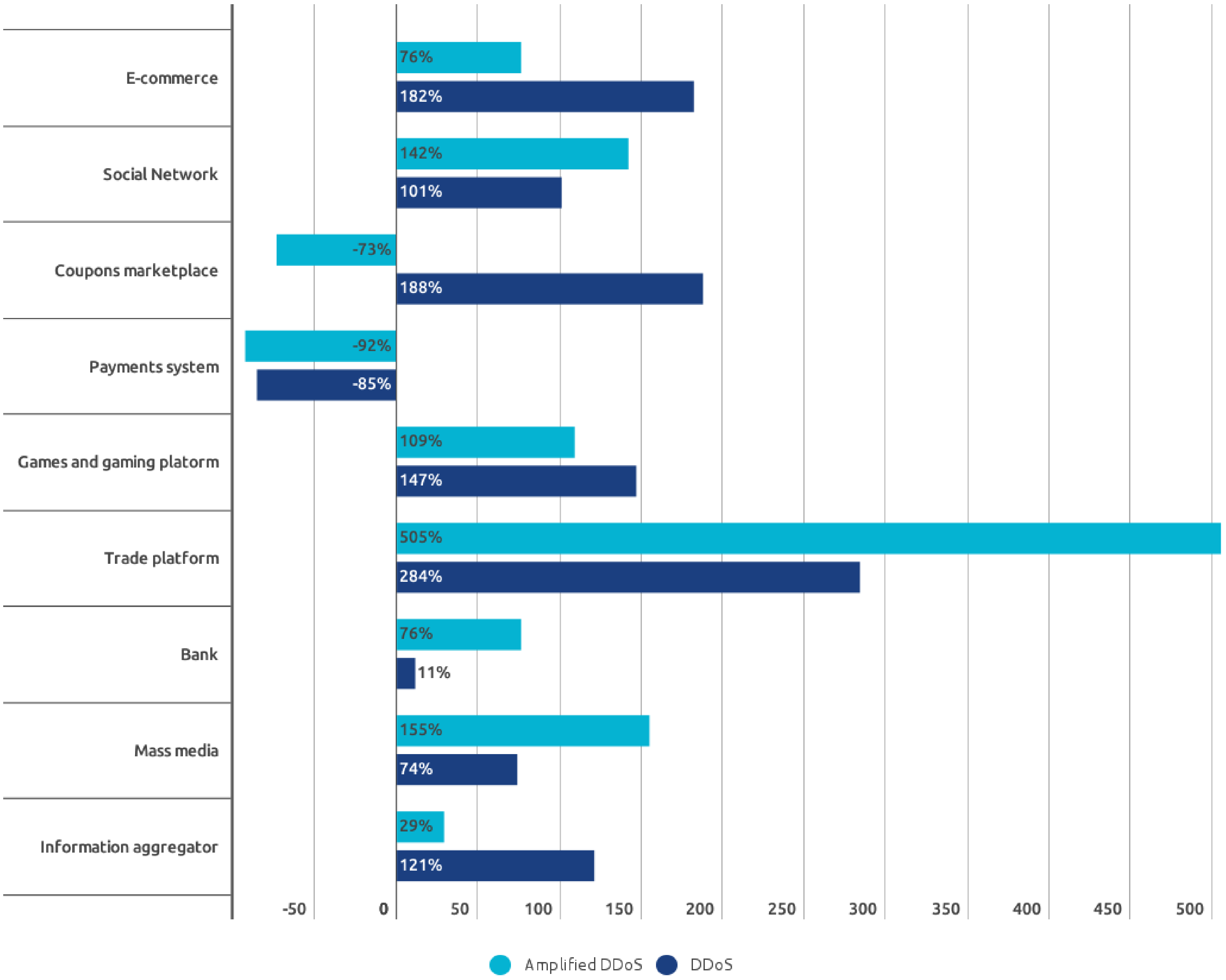
```
21:30:01.226808 IP 77.109.59.88 > 178.248.233.141: GREv0, length 544: IP 177.29.144.71.1794 > 233.40.195.59.80: UDP, length 512
21:30:01.226818 IP 188.227.49.37 > 178.248.233.141: GREv0, length 544: IP 74.8.210.201.62170 > 114.236.221.61.80: UDP, length 512
21:30:01.226827 IP 188.116.128.35 > 178.248.233.141: GREv0, length 544: IP 207.175.156.190.25403 > 13.231.228.114.80: UDP, length 512
21:30:01.226836 IP 176.110.8.249 > 178.248.233.141: GREv0, length 544: IP 33.224.192.129.35165 > 125.67.17.104.80: UDP, length 512
21:30:01.226841 IP 79.111.173.31 > 178.248.233.141: GREv0, length 544: IP 98.93.53.156.38682 > 71.199.184.195.80: UDP, length 512
21:30:01.226845 IP 37.235.165.54 > 178.248.233.141: GREv0, length 544: IP 148.62.64.254.2786 > 0.90.178.37.80: UDP, length 512
21:30:01.226846 IP 89.22.255.63 > 178.248.233.141: GREv0, length 544: IP 105.116.87.79.16544 > 191.208.81.56.80: UDP, length 512
21:30:01.226847 IP 94.140.231.52 > 178.248.233.141: GREv0, length 544: IP 202.237.76.156.22900 > 166.36.94.118.80: UDP, length 512
21:30:01.226857 IP 62.122.241.17 > 178.248.233.141: GREv0, length 544: IP 130.167.72.47.7434 > 71.27.233.141.80: UDP, length 512
21:30:01.226863 IP 94.251.116.51 > 178.248.233.141: GREv0, length 544: IP 184.224.242.144.24333 > 74.206.4.88.80: UDP, length 512
21:30:01.226865 IP 176.104.207.150 > 178.248.233.141: GREv0, length 544: IP 105.6.191.235.16488 > 12.95.159.63.80: UDP, length 512
21:30:01.226867 IP 188.43.110.176 > 178.248.233.141: GREv0, length 544: IP 137.194.5.192.64457 > 229.206.83.2.80: UDP, length 512
21:30:01.226868 IP 94.251.116.51 > 178.248.233.141: GREv0, length 544: IP 184.224.242.144.65323 > 167.42.221.164.80: UDP, length 512
21:30:01.226873 IP 46.227.212.111 > 178.248.233.141: GREv0, length 544: IP 90.185.119.106.50021 > 179.57.238.88.80: UDP, length 512
21:30:01.226881 IP 46.39.29.150 > 178.248.233.141: GREv0, length 544: IP 31.173.79.118.42580 > 115.108.7.79.80: UDP, length 512
21:30:01.226884 IP 62.122.241.17 > 178.248.233.141: GREv0, length 544: IP 130.167.72.47.28623 > 206.51.246.56.80: UDP, length 512
21:30:01.226884 IP 80.237.121.124 > 178.248.233.141: GREv0, length 544: IP 2.38.197.44.62074 > 29.78.78.210.80: UDP, length 512
21:30:01.226886 IP 46.227.212.111 > 178.248.233.141: GREv0, length 544: IP 90.185.119.106.62374 > 140.224.35.149.80: UDP, length 512
21:30:01.226888 IP 188.94.34.112 > 178.248.233.141: GREv0, length 544: IP 79.54.127.3.54141 > 163.108.94.204.80: UDP, length 512
21:30:01.226888 IP 94.140.231.52 > 178.248.233.141: GREv0, length 544: IP 202.237.76.156.29729 > 4.110.54.239.80: UDP, length 512
21:30:01.226890 IP 80.237.121.124 > 178.248.233.141: GREv0, length 544: IP 2.38.197.44.55671 > 188.160.65.128.80: UDP, length 512
21:30:01.226890 IP 213.27.82.105 > 178.248.233.141: GREv0, length 544: IP 149.69.25.193.39138 > 143.158.0.201.80: UDP, length 512
21:30:01.226892 IP 89.22.255.63 > 178.248.233.141: GREv0, length 544: IP 105.116.87.79.15913 > 169.150.19.75.80: UDP, length 512
21:30:01.226893 IP 46.39.29.150 > 178.248.233.141: GREv0, length 544: IP 31.173.79.118.64845 > 213.6.185.81.80: UDP, length 512
21:30:01.226895 IP 37.131.203.235 > 178.248.233.141: GREv0, length 544: IP 60.19.226.97.45868 > 104.3.54.144.80: UDP, length 512
21:30:01.226895 IP 79.111.173.31 > 178.248.233.141: GREv0, length 544: IP 98.93.53.156.23695 > 227.223.153.67.80: UDP, length 512
21:30:01.226896 IP 77.109.59.88 > 178.248.233.141: GREv0, length 544: IP 177.29.144.71.19901 > 40.154.105.240.80: UDP, length 512
21:30:01.226897 IP 176.110.8.249 > 178.248.233.141: GREv0, length 544: IP 33.224.192.129.46814 > 65.200.67.203.80: UDP, length 512
```

September 20, 2016: KrebsOnSecurity.com becomes the target of a record-breaking 620 Gbps volumetric DDoS attack from a botnet designed to take the website down.
The Mirai bot includes several layers of attack in its arsenal: standard SYN floods, TCP floods, and UDP floods. These vectors could typically be mitigated either at a cloud scrubber or, if they are sufficiently small, at the network defense tier in the data center.

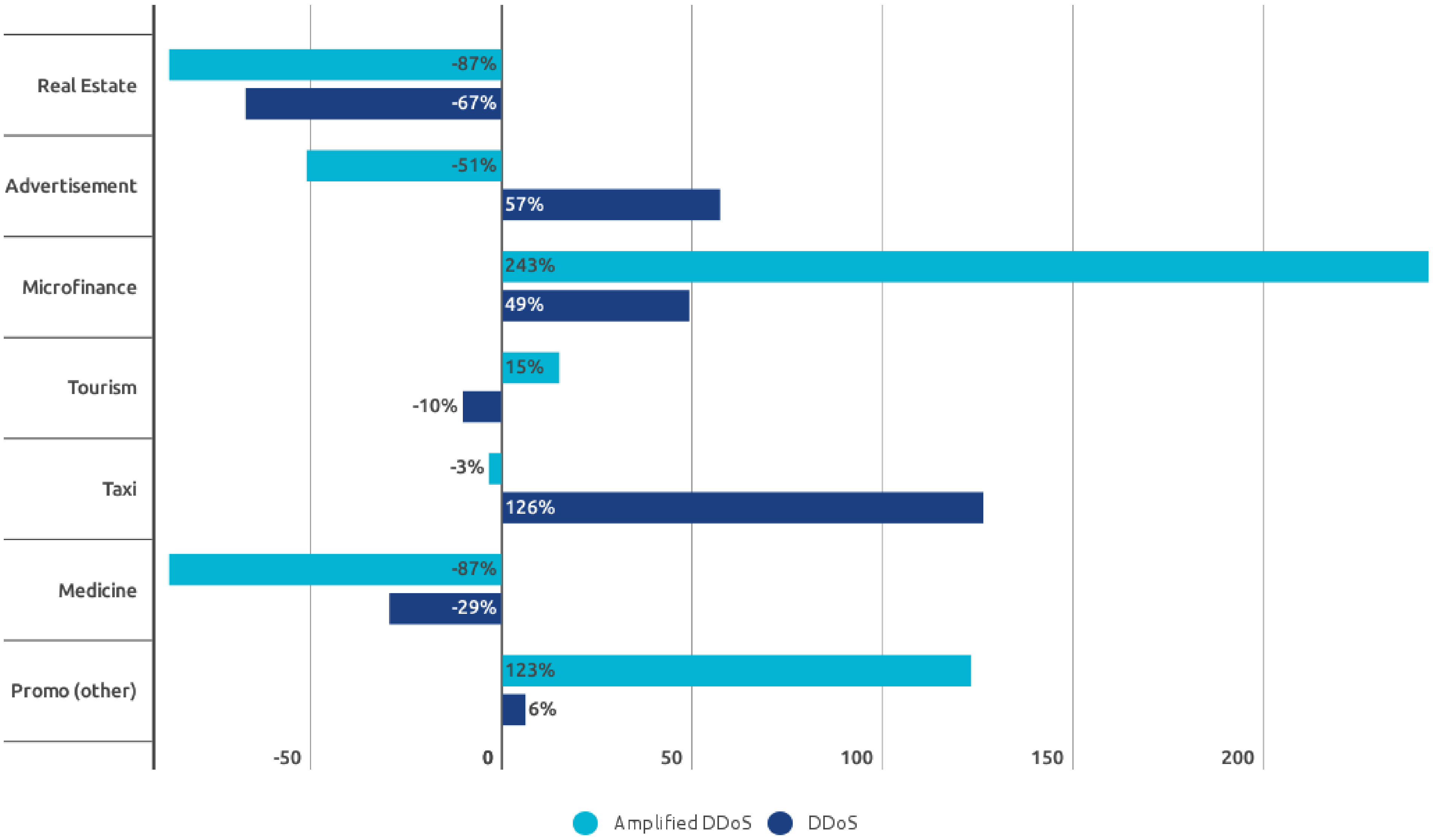
September 21, 2016: The same type of botnet is used in a 1 Tbps attack targeting the French web host OVH. A few days later, the IoT botnet source code goes public — spawning what would become the
“marquee” attack of the year.
OVH was hit with a volumetric attack of 990 Gbps. There were reports that the Dyn attack peaked at 1.2 Tbps.

October 21, 2016: Dyn, a US-based DNS provider that many Fortune 500 companies rely on, is attacked by the same botnet in what is publicly known as a “water torture” attack.
The attack has been described as a complex & sophisticated issue, using maliciously targeted TCP and UDP traffic over port 53 from more than 100,000 endpoints.

Industries perspective, yearly (2015 - 2016) attacks dynamics percentage



More details on promo-sites



All industries suffer from DDoS attacks — Internet is everywhere

DDoS attacks and incidents came back to the scene during 2016 at full strength, though to some observant earlier it started to seem like the entire issue had gone away. The latter stood because of the most damaging attacks of the past - amplification attacks - were easy to mitigate for a large ISP, even when attack strength started to reach figures like 100 to 300 Gbps. Also, other complex types of attacks, like sophisticated L7 ones, rather rarely happened in past years.

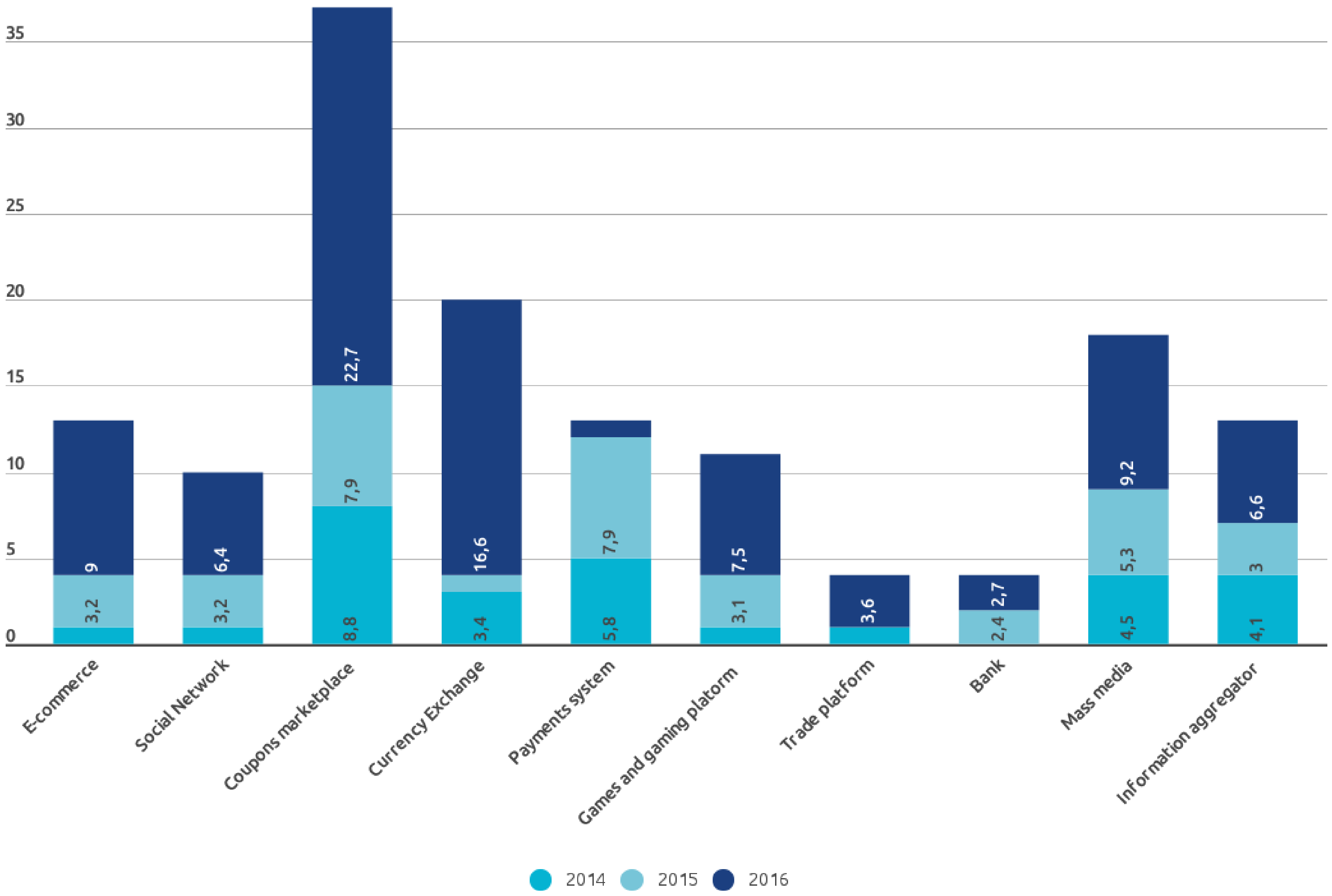
One fact was the most interesting to us: all those devices — web- cameras, DVRs, some sim-enabled devices — had vulnerabilities which were exploited on such a high scale in such a short time. End of 2016 was an unusual period when all those DDoS risks again made the front page of every media outlet. **Just like 5, 6, or 7 years ago all technical experts, again, have to pay attention to DDoS mitigation.**

In recent years we saw linear peak growth in DDoS attacks, but 2016 showed predictable growth of attacks depending on where those land to. Now we can seriously discuss offensive capabilities dangerous for the whole regions of the world availability in general, large ISPs' capacity to function at all.

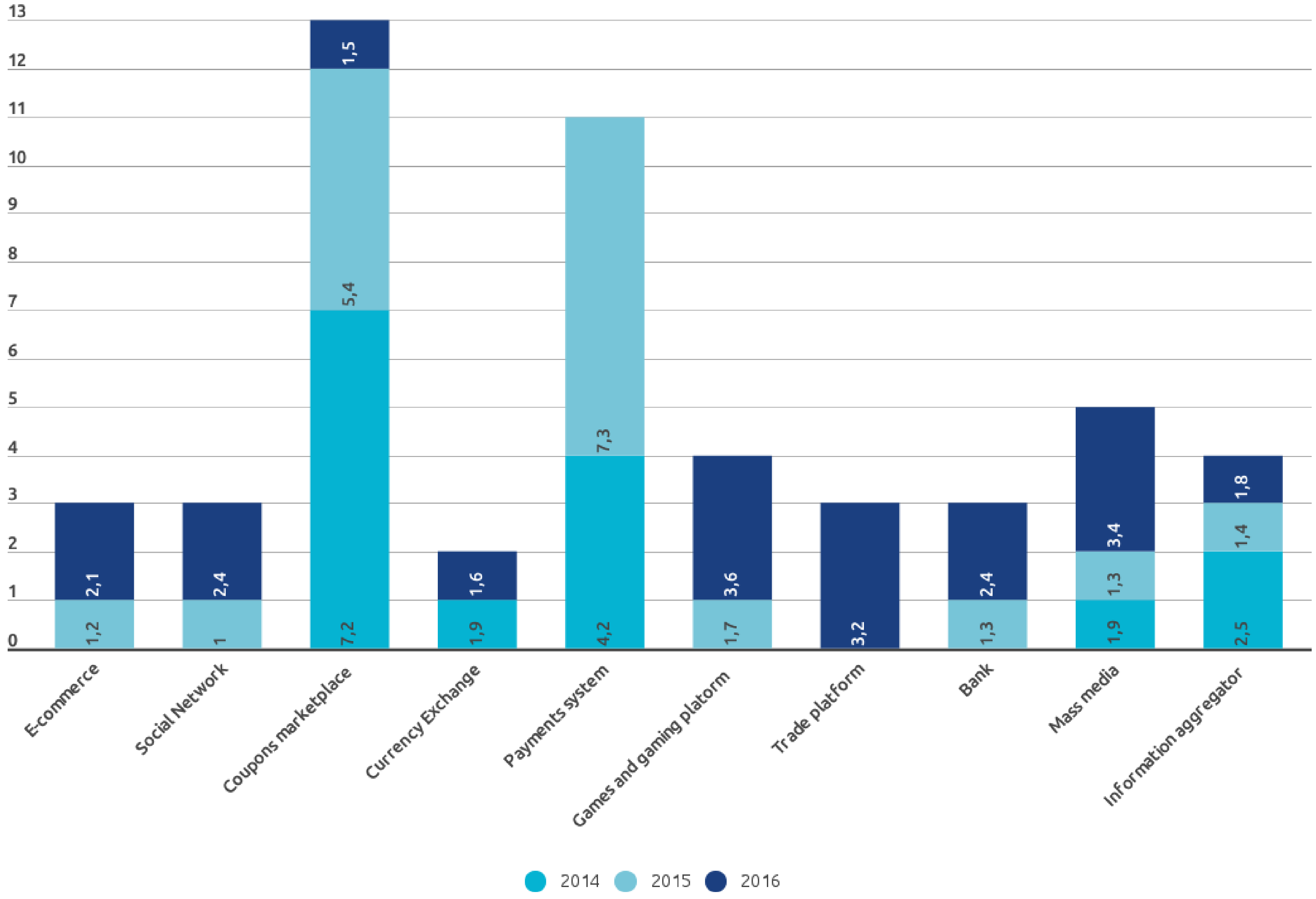
A cleverly distributed DoS attack may once again reach and exceed 1 Tbps in 2017

"What do these attack show? The entire IT evolution during these years was a race against time and competitors. Cut the corner at the right time and place — and you are the winner. However, regarding how today's internet works, from protocol specifications to the actual implementations of specific applications and services, the technical debt has to be paid."

DDoS activity by industry, three-year perspective



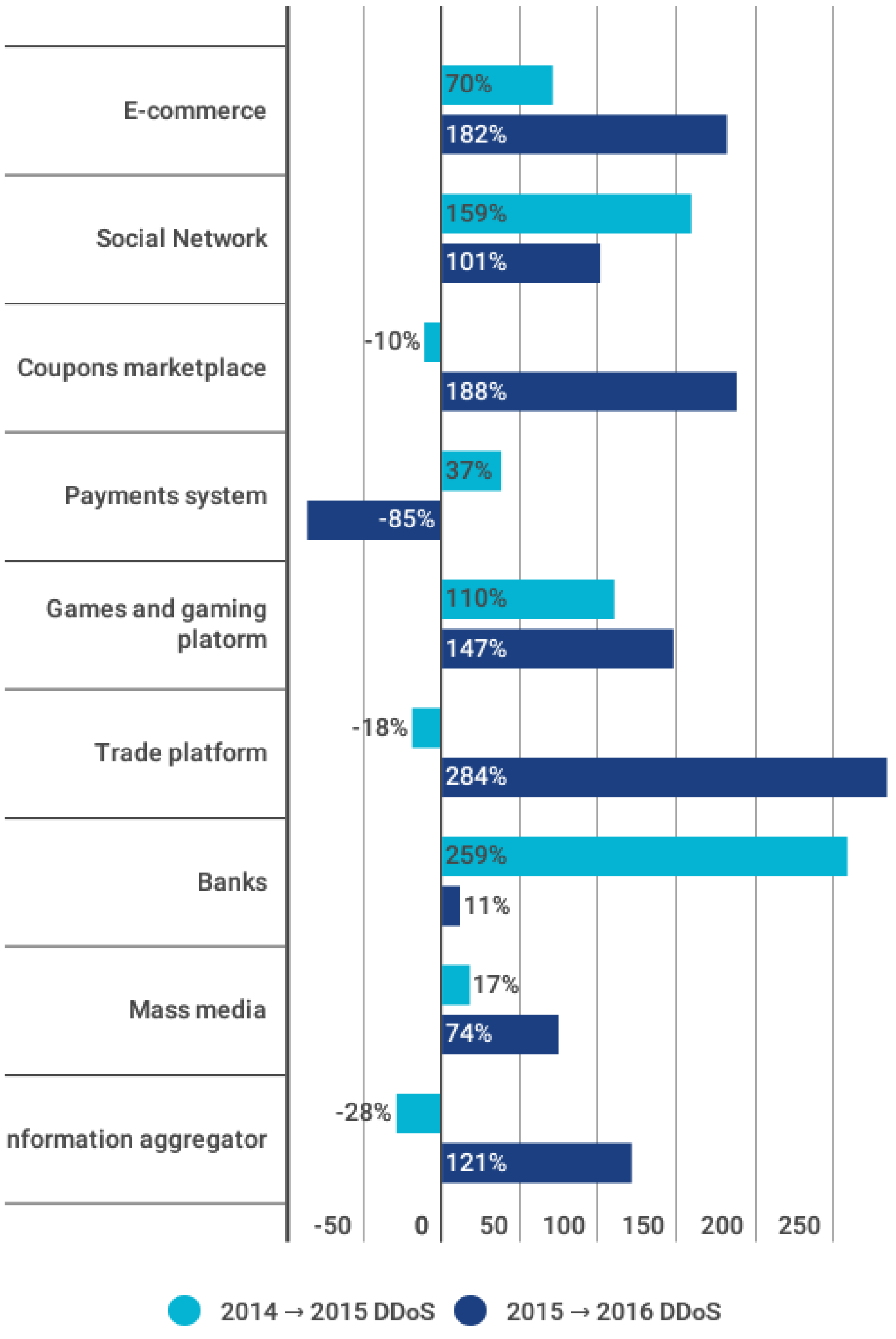
Amplified DDoS activity overview



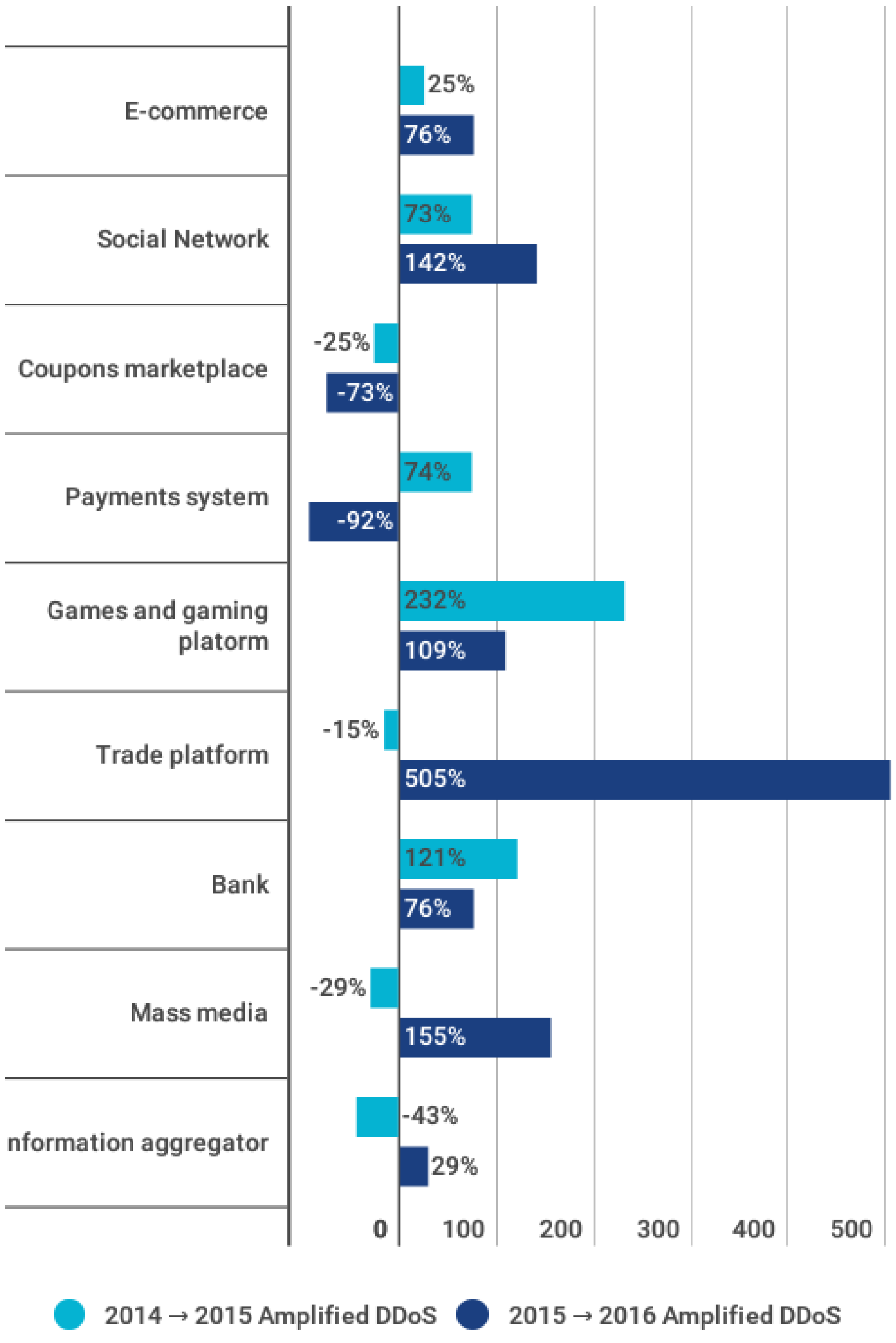
An ongoing network transformation

2014 - 2016 DDoS Dynamics Overview

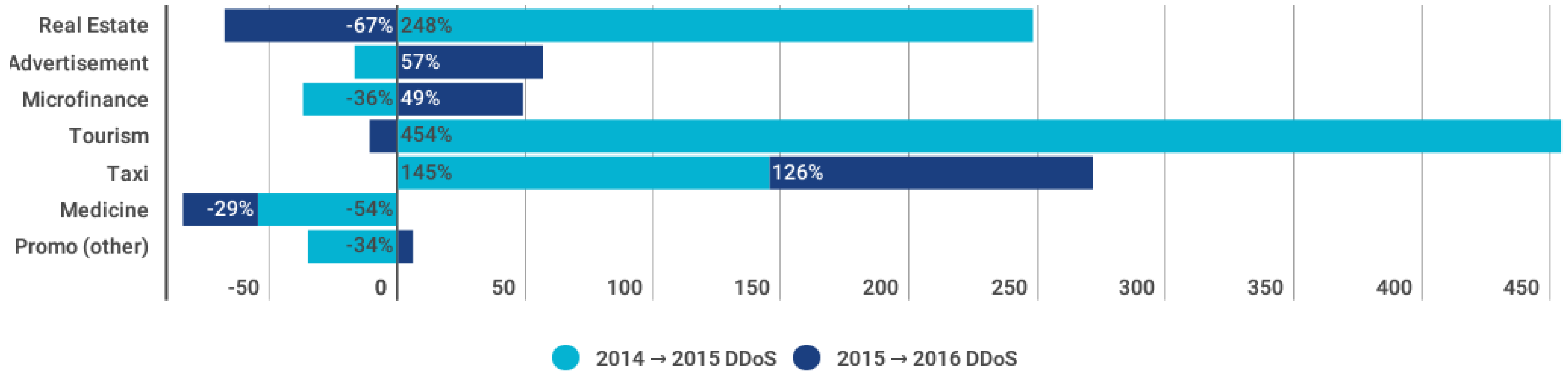
DDoS 2014 - 2016

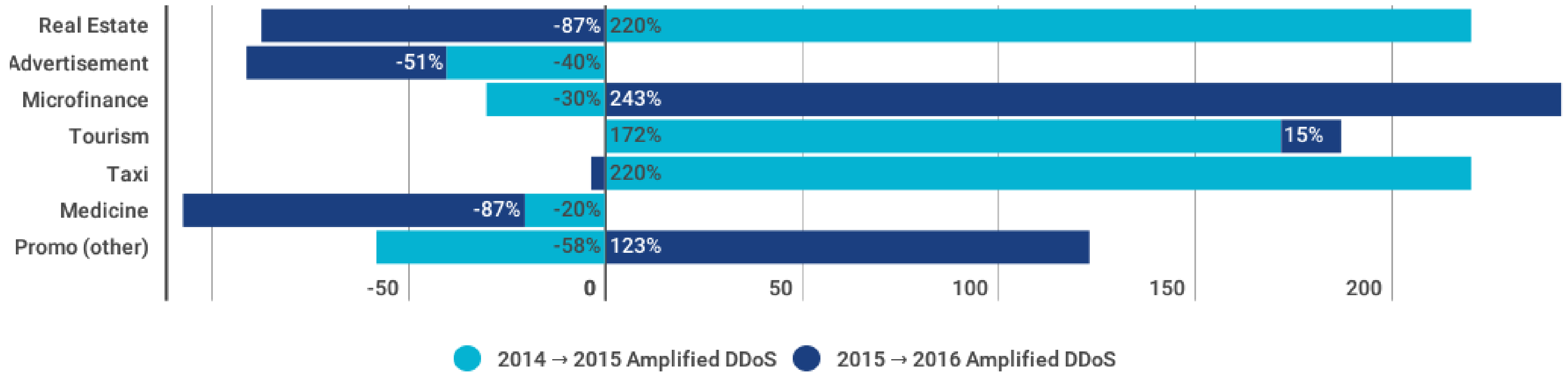


Amplified DDoS 2014 - 2016



Promo-sites details



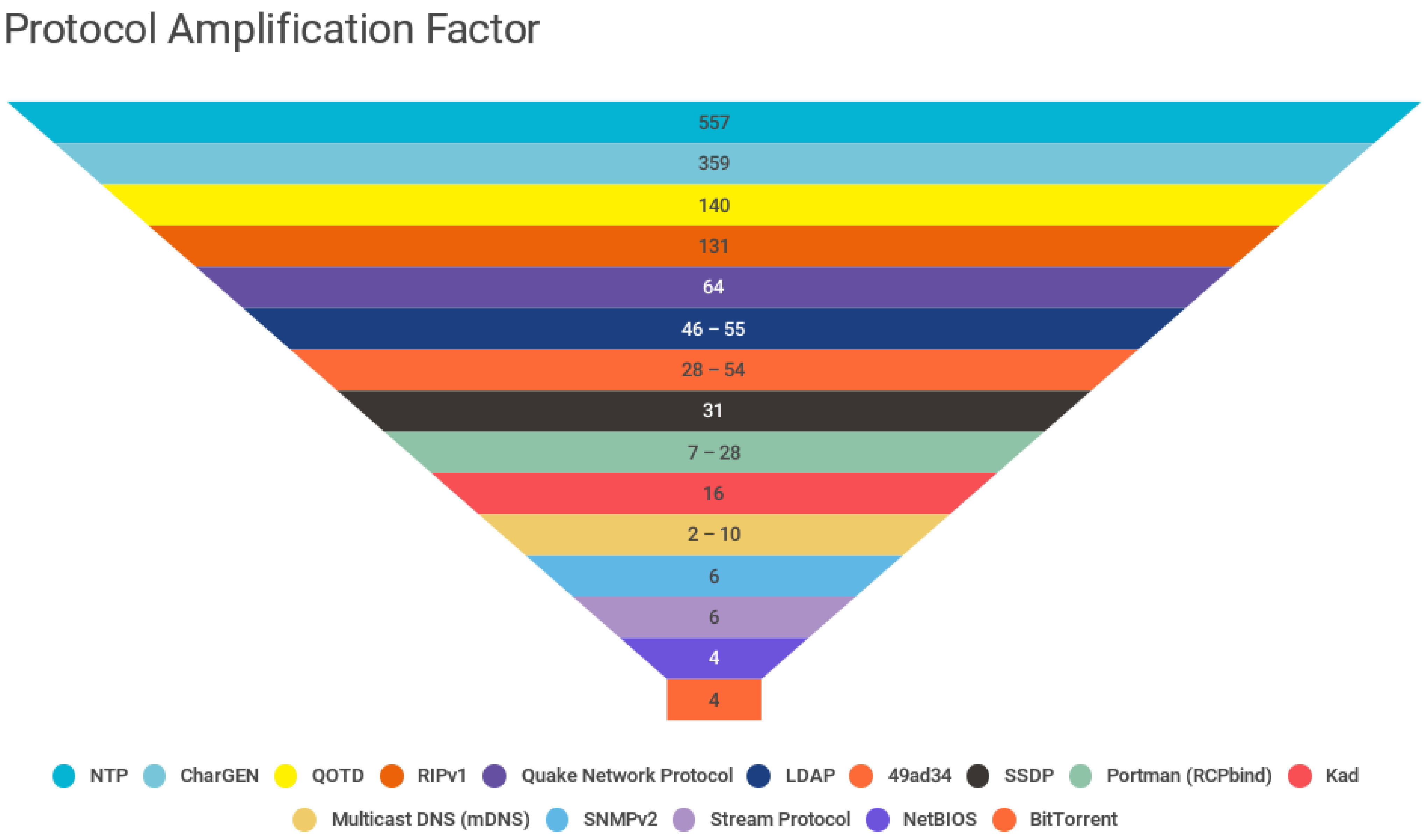


The first victim of the race for the price is security. It is often omitted to achieve desired product at competitive cost. That is why modern network infrastructure is so hard to protect from cyber attacks, and actually, there is no reason to think that this would change at some intermediate term. We believe that with the startup boom there would be even more companies that take shortcuts while developing their products — and it would affect the Internet as a whole.

A Mirai-associated threat is not something unique, and Imperva Incapsula already registered a 650 Gbps attack from Leet botnet with two different SYN payloads. **As we mentioned earlier, at Qrator Labs we are confident that Mirai is only the first child from a whole generation of IoT botnets, which we would observe during the year 2017.** Even solving the Mirai problem these days would not help — as we would explain further, changes are tectonic.

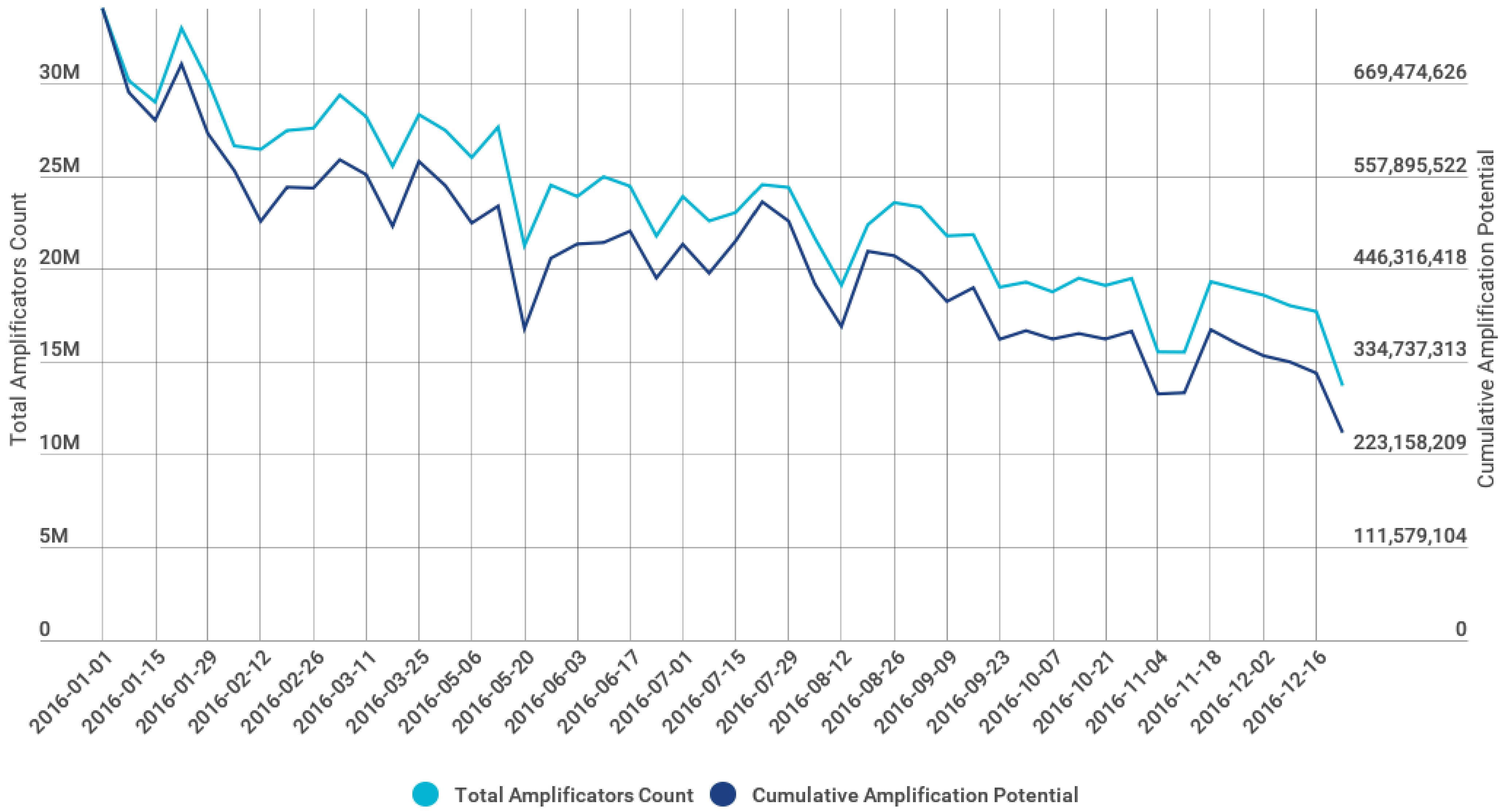
Overseeing Internet infrastructure, we record the lack of essential security part. These days it is enough to attract individuals willing to make profits out of existing bugs and vulnerabilities. Vacuum is never empty.

Economics are merciless, and the price is a king



> Infrastructure attacks became possible because people and technical specialists fear of what's scary, not what's dangerous.

Amplificators and Amplification decline over 2016



Over the past few years, HTTP has been the most exploited protocol, and eventually, it has become the most protected as well. People have got to know either how to mitigate or at least where to seek protection.

Infrastructure, like DNS, only recently has started to be a real target of cyber-attacks, and it is still insecure.

The usual way to mitigate an HTTP-based amplification attack relies on source-port analysis (53, 123../) — only 10 of them are commonly used, peculiarly we never see those in the legitimate traffic. On the contrary, during an attack on DNS server 53 port could not be blocked or there would occur an availability issue.

So that is why DNS amplification attacks should be processed. However, in the real world, where 40 Gbps upstream and a significant CPU power is needed to do so, even the biggest companies rarely do that — they do not have the bandwidth, and they lack wire speed packet handling because DNS does not require it.

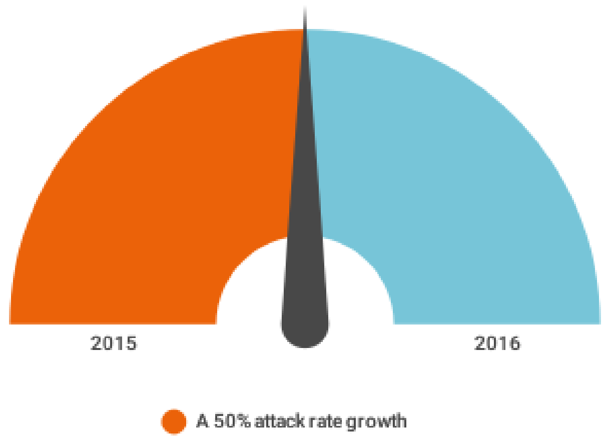
Which amusingly still doesn't matter, because a Mirai-associated botnet could generate any type of junk traffic, including this DNS amplification one, looking legitimately. The only reason of such botnet evolution is that villains found sore points at the infrastructure.

So the year 2016 revealed that a well-oriented infrastructure attack could deal enormous collateral damage to all connected applications and services, companies, dependable on any of those technologies.

ISPs and network operators solve their own problems, not customer’s

What we saw in the ISP world, where the customer is limited by strict agreement on DDoS mitigation solutions, is that an ISP is not going to protect its customer at all costs. **After a DDoS bandwidth reaches some boundary and other customers begin to suffer, the ISP would use the Blackhole Community to drop everything towards the attacked service, or could simply abandon the service**, as Akamai with Prolexic did with Brian Krebs when he was attacked for his work.

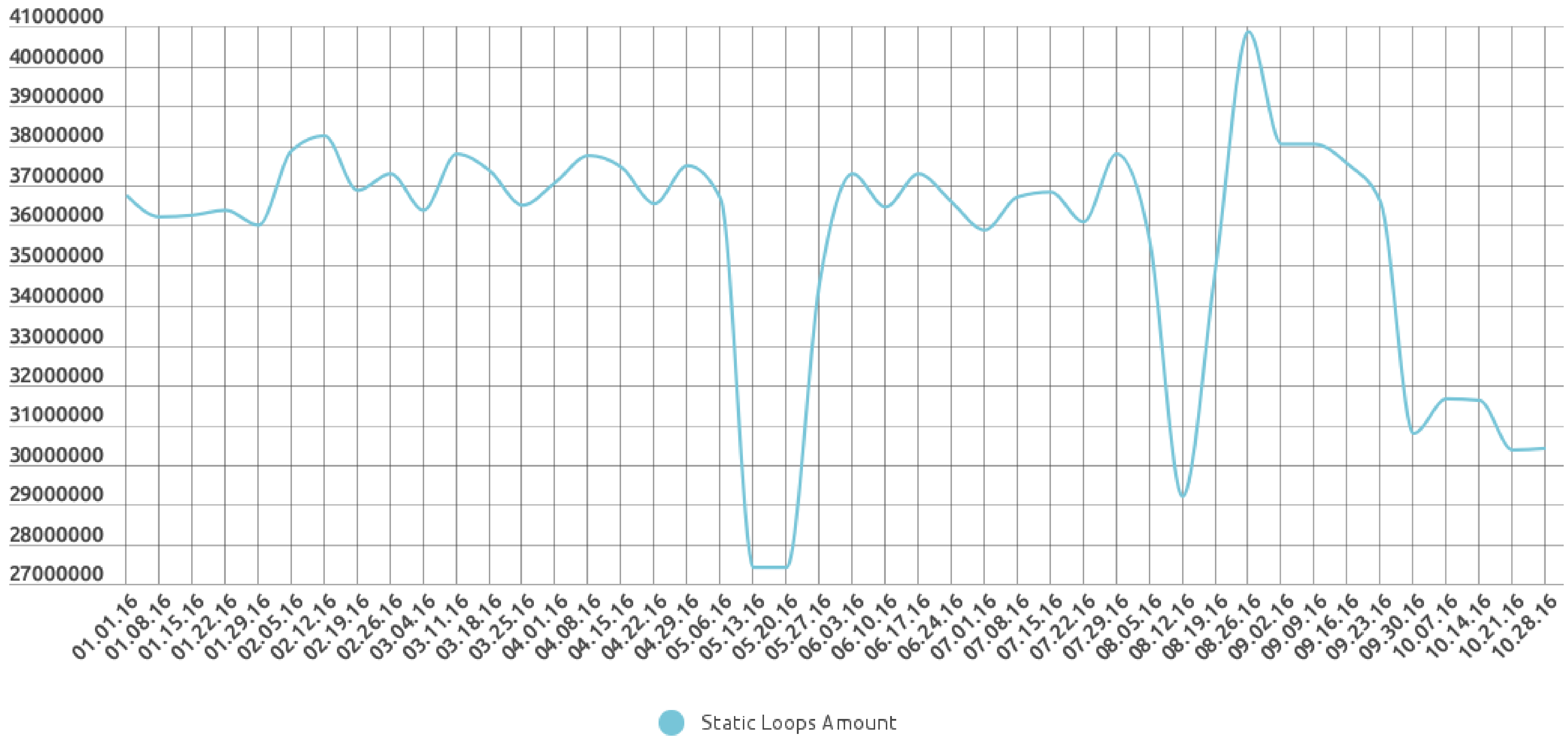
Year to year attack rate growth



While speaking about the operators themselves, it is still rather easier for them to survive attacks unless we are talking about cyber extortion. The income would not fall low because a couple of clients were lost. However, when the criminal prepared enough to successfully attack an ISP would endanger the business itself, we cannot predict what a threatened company is going to do in this case. That might be the risk of 2017, but as we see this now — criminals choose other than ISP businesses as primary targets.

In our practice, we often come across a peculiar fact: many clients use multiple mitigation solutions. A cascade of protection layers should perform better according to these customers' logic. **However, a layered defense may backfire.** After switching DDoS mitigation services providers, you have to be certain the previous one does not work with you anymore. BGP makes it highly complicated to tell where those /25 prefixes could be routed, where they could become “more accurate,” and who else could be affected.

Static loops in 2016

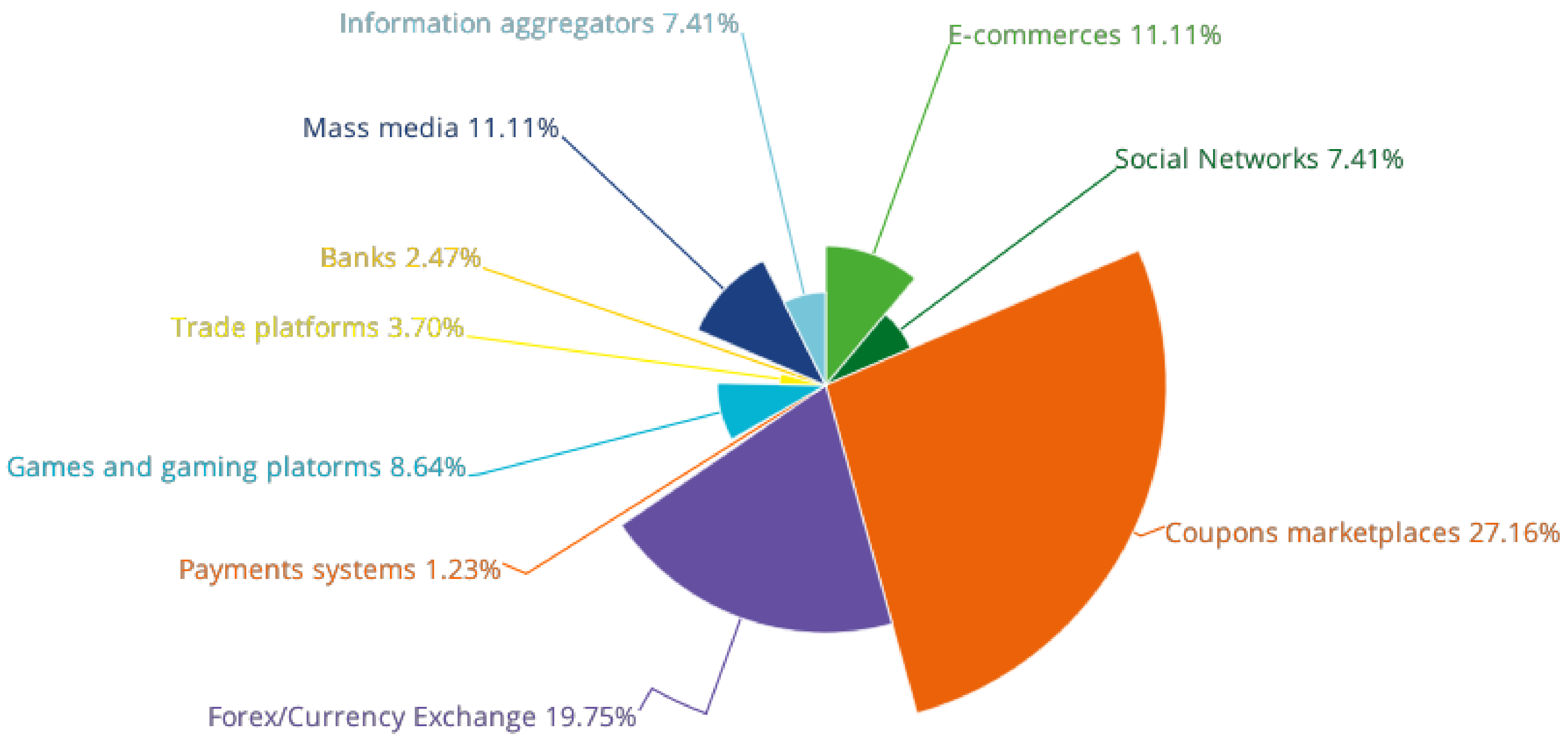


Next: Statistics & Specifications

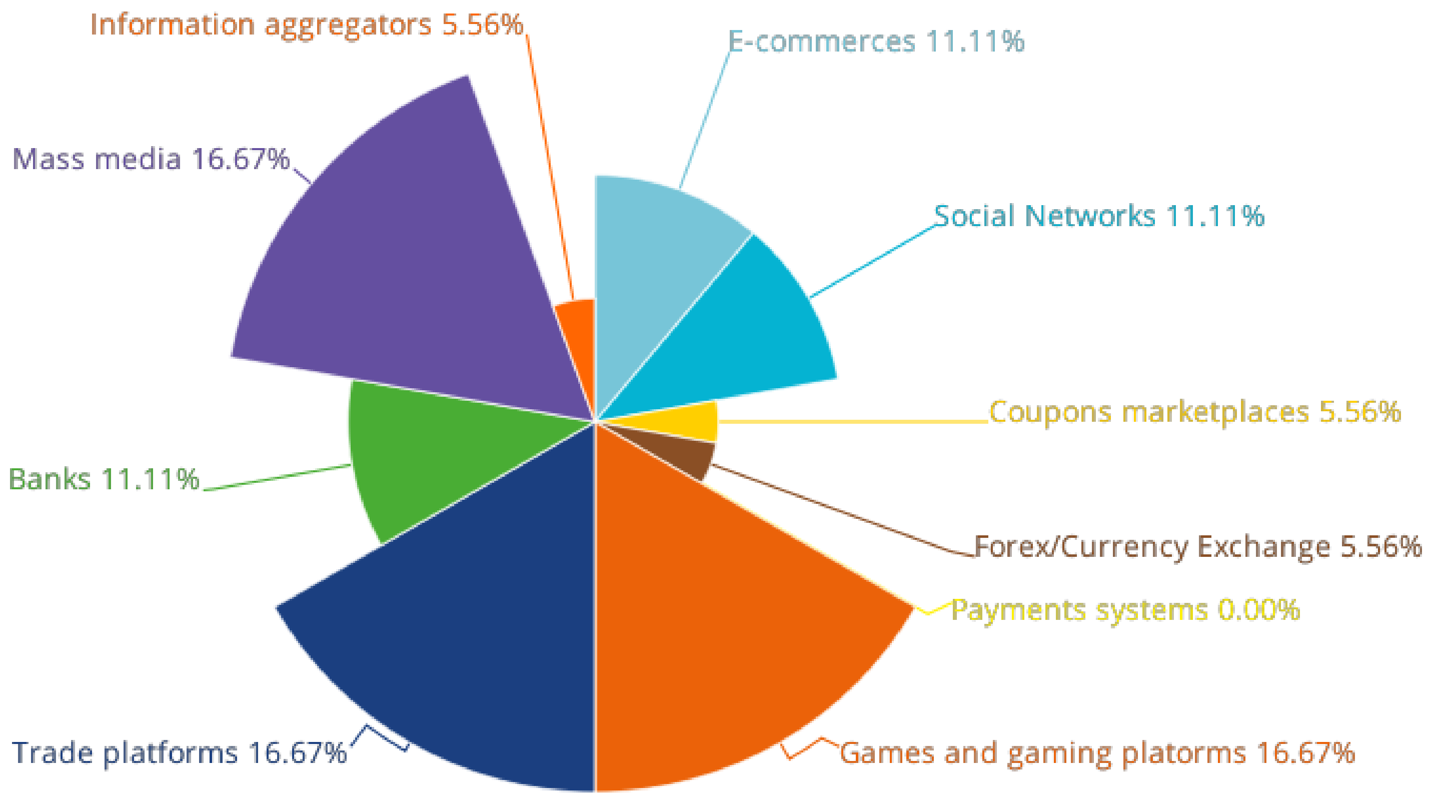
3. Statistics and Specifications

Yearly DDoS vs. Amplification DDoS attacks ratio percentage

All DDoS attacks



Amplification DDoS attacks



Underlying Internet infrastructure is fragile and needs update, as well as investments of time, money and effort

Internet measurement and analytics

BGP was introduced in late 80's as a napkin draft made by 3 engineers. Consequently, it answered the questions related to that era. The BGP logics says, “pick the best route available,” which may be quite different from the logics of organizations operating these border gateways. **Money comes first as usual.** If financial matters say it is cheaper to send traffic on a trip from one country to another and then back in the same country, any ISP would do so without hesitation.

Not only this is a latency issue - the ISPs could profit if they establish peering relations. With proper peering in case, any sort of problems occurs, they could be resolved directly, not through some 3rd party. However, politics come into the equation again. Some ISPs did not, do not, and would not peer with each other, ever.

The problem of poorly organized infrastructure did not come up in 2016, and it was evident both in 2015 and 2014. The core Internet infrastructure is, and always was based on trust, but some people making hasty and dissatisfactory decisions cannot be trusted.

The way the core Internet infrastructure is financed is subpar. It does not comply and goes up to date with the current cadence of the Internet evolution.

Speaking about BGP, the biggest problem with it right now is that it does not do any checks on the routing data it operates on by default. It does not enforce verification of any routing information. All BGP problems arise here. The protocol leaves a lot of breaches, which could generate mistakes, or just be exploited by malefactor or criminal. **So that is the point where hijacking issue originates from, as well as route leaks and bogon routes**: BGP does not bother to verify the route and answer a simple question of “does this path exist and is it legitimate?”. It just transmits the routing data (with few modifications).

BGP routing issues are hard to find and resolve because route propagation is out of control from a single ISP

"Routing issues are quite specific for our customers. For example, Internet traffic between two arbitrary locations in Russia may cross the border and go through other parts of Europe on a regular basis, which would affect both Russian and European customers."

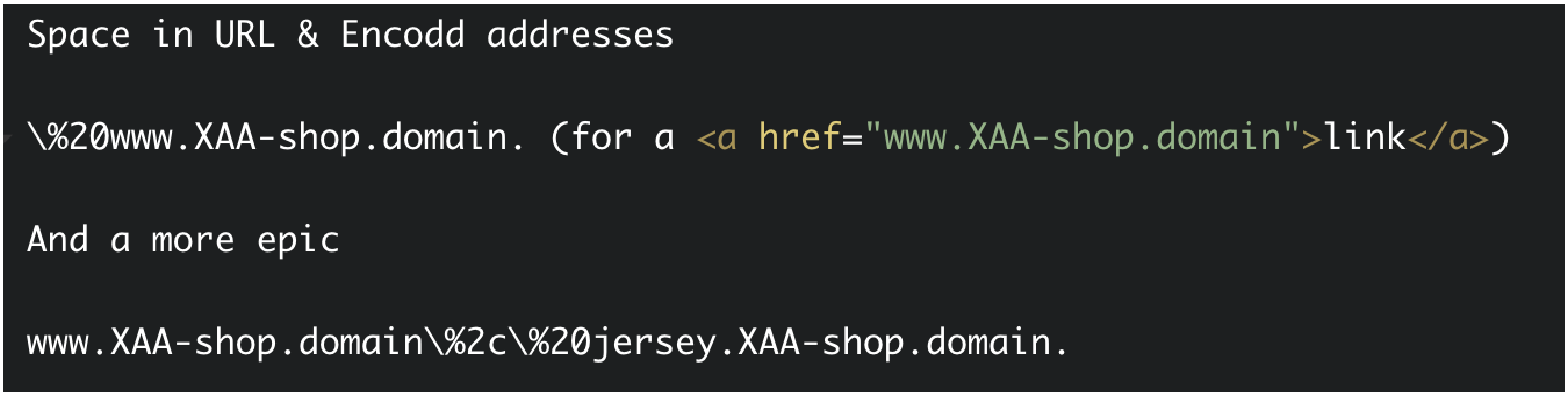
Cloud management

Why do clouds not fail? They did not fail up to this moment just because in the case of emergency any client would be shut down before any serious problems may occur

Even when the cloud appears to be powerful enough to allocate all the resources necessary for handling all the unsolicited requests, it will sooner or later cut the service to its customer when the bill grows too much. Considering severe discounts on booter services that could be a serious problem for Internet businesses all over the world next year.

With "hit and run" tactics where we observe mainly short though frequent attacks.

Some cloud platforms promise not to charge their customers for the resources consumed during DDoS attacks. However, this refers to volumetric attacks only. When a client is under a volumetric attack, which is, in most cases, amplification attack, it is quite easy for them to prove it, and it is easy as well for the cloud to mitigate it with modern techniques like BGP FlowSpec. However, a sophisticated application-level attack is almost indistinguishable from the legitimate traffic, and it gets billed. DDoS mitigation, once again, does not come for free here.



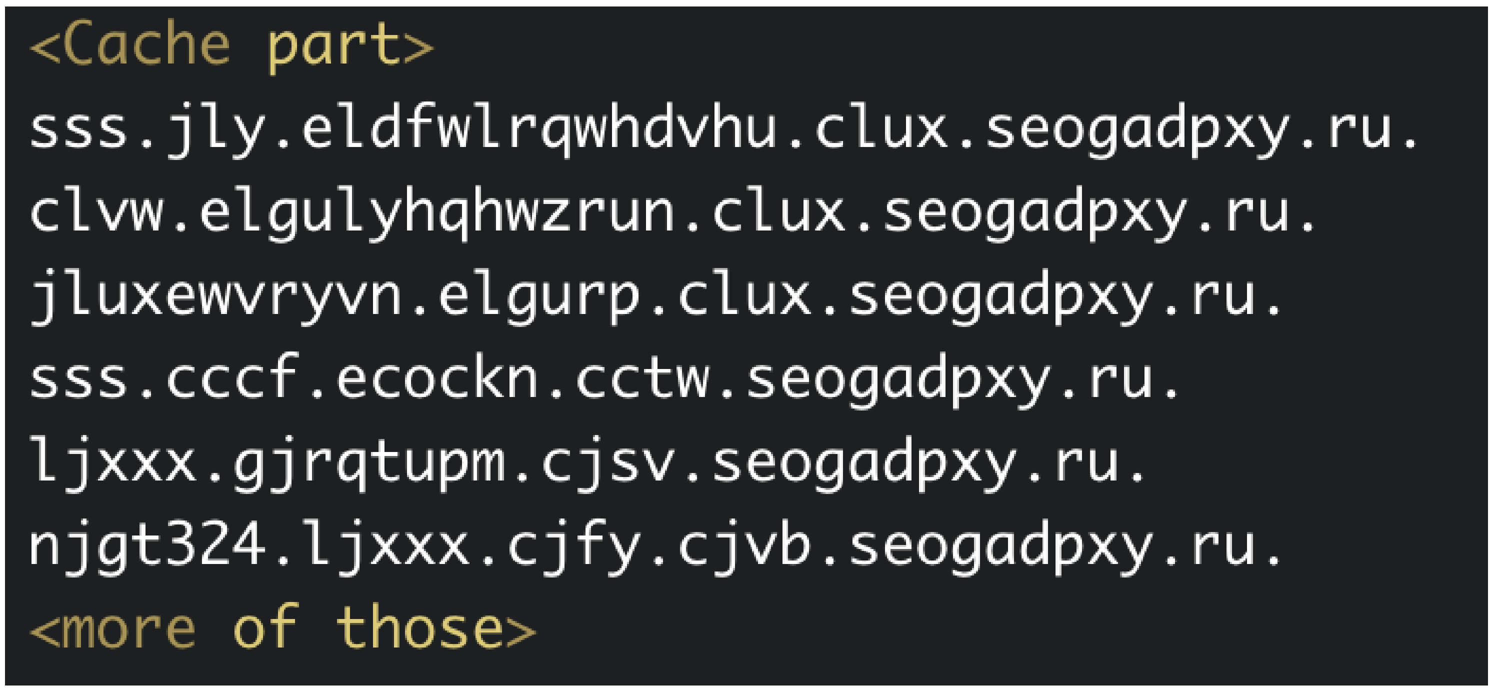
```
Space in URL & Encodd addresses

\%20www.XAA-shop.domain. (for a <a href="www.XAA-shop.domain">link</a>)

And a more epic

www.XAA-shop.domain\%2c\%20jersey.XAA-shop.domain.
```

Google tells there was an anonymizer at some time, which is inactive, but the cache record is recent



```
<Cache part>
sss.jly.eldfwlrqwhdvhu.clux.seogadpxy.ru.
clvw.elgulyhqhwzrun.clux.seogadpxy.ru.
jluxewvryvn.elgurp.clux.seogadpxy.ru.
sss.cccf.ecockn.cctw.seogadpxy.ru.
ljxxx.gjrqtupm.cjsv.seogadpxy.ru.
njgt324.ljxxx.cjfy.cjvb.seogadpxy.ru.
<more of those>
```

3.1 Infrastructure

IPv6 is a parallel network

People are slow to integrate IPv6 mainly because they do not know how to handle it. For example, they tend to think that NAT absence in IPv6 could make things worse.

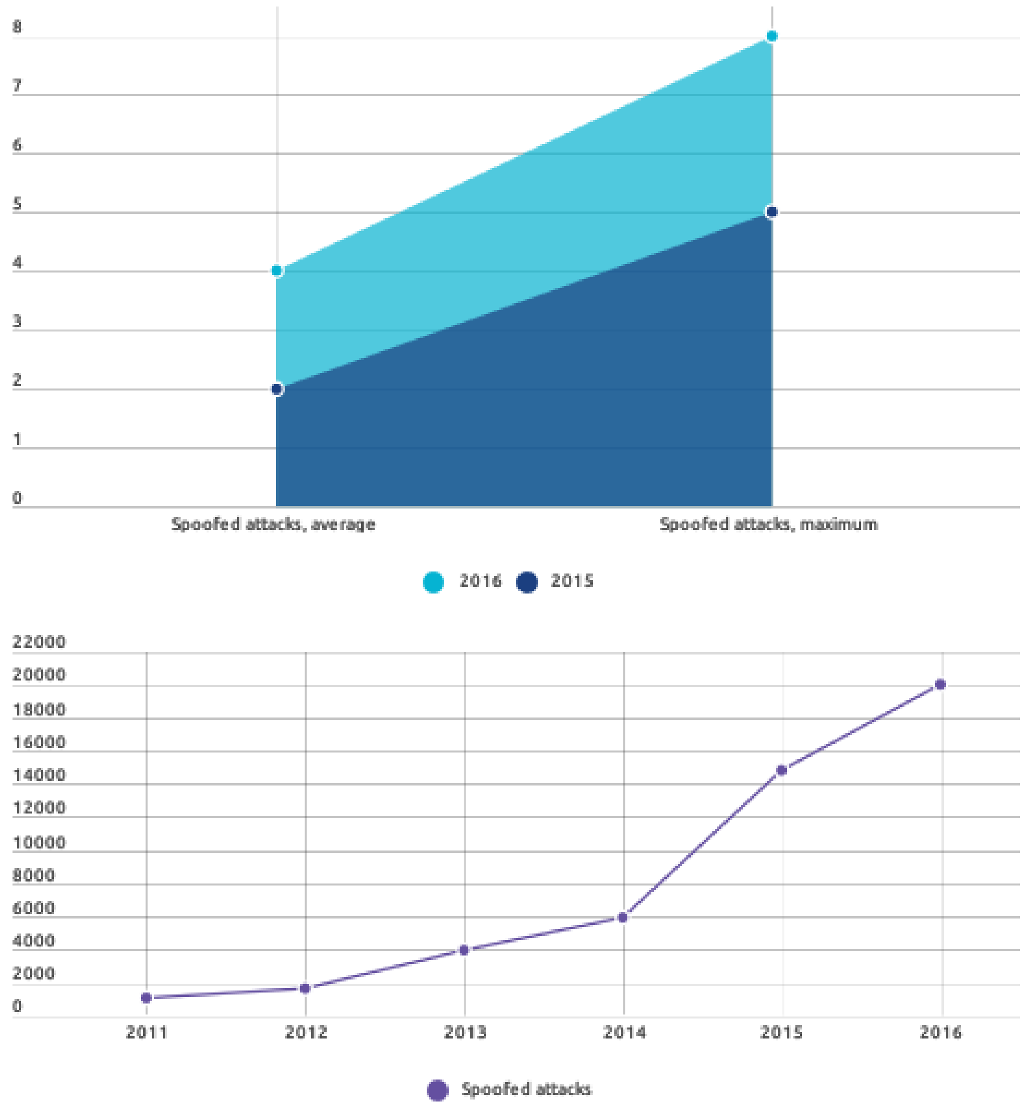
However, the only thing that NAT does in IPv4, regarding security, is stateful connection tracking, and in IPv6, firewalls can do it as well. **Lack of knowledge in this field leaves us with "professionals" who do not realize the necessity of tracking connections, consciously blocking unsolicited access to the system — you do not need NAT for that.**

The IPv6 protocol stack itself is rather effective in the way of routing and packets are exchanged, except for few problems with data structures for IPv6 address storage. IPv6 addresses have an excessive length, and that may be an issue for those trying to store large portions of the address space for tracking or filtering purposes. However, everything else — the firmware code we have in routers, the methodology of tech support, and problem solution within large enterprises and among ISPs' clients — is in a sad state.

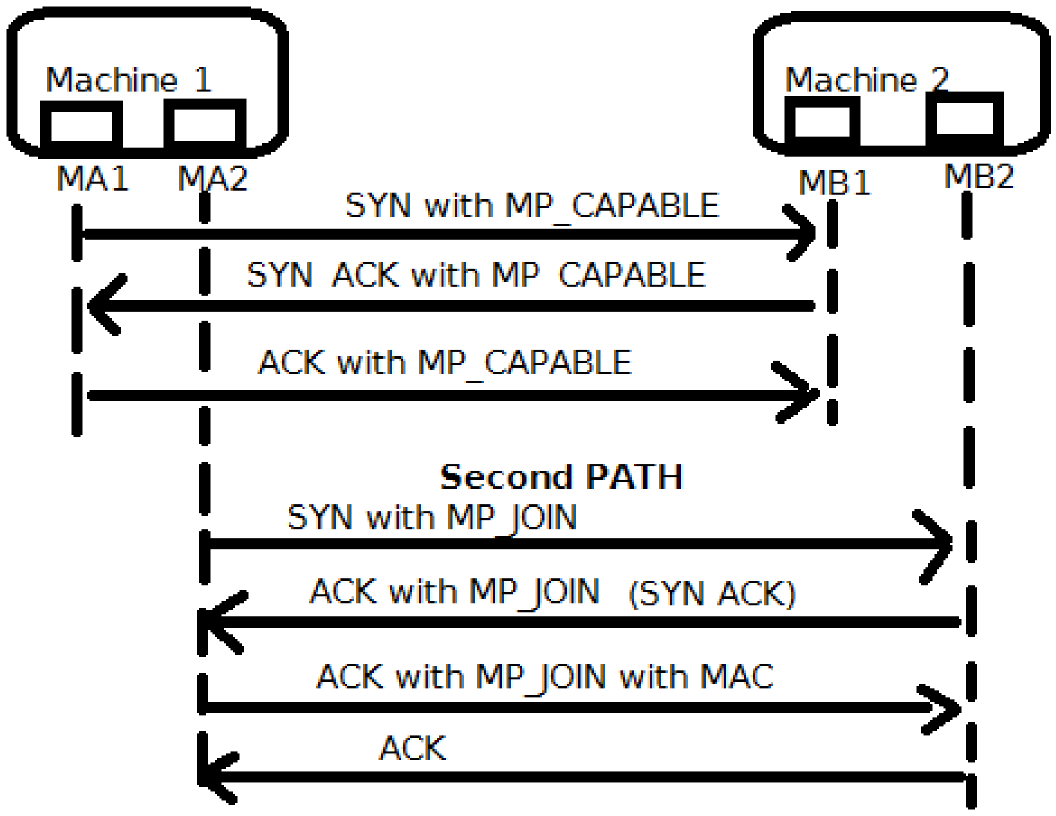
Lots of pros at technical operations and maintenance admit that when they notice some problem in their network, they just shut down the v6 system. In 55-60% of cases, this solves the problem. Does it? Obviously, it does not.

IPv6 was introduced in such a hurry partly because of the v4 address pool exhaustion. Global address pool exhaustion could be a huge problem if the industry ignored the issue, but now that is probably not the weakest point.

Average spoofed attacks 2015 - 2016 vs. year by year amount



MPTCP explanation scheme

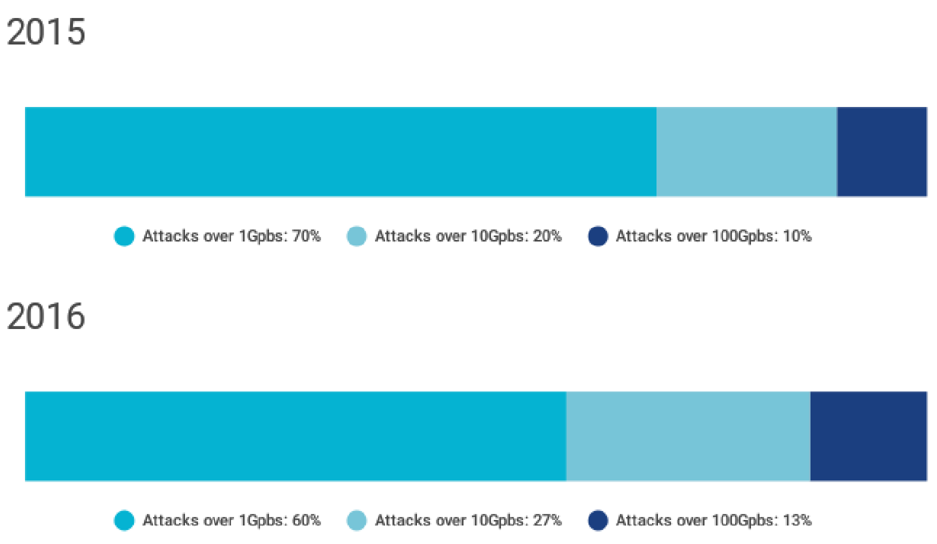


Probably the best way to introduce IPv6 at your organization nowadays is to do this in a limited environment or a sandbox

Engineers have to get used to it, while it may be too early to rely on it very much: the protocol would attract some attention from the dark side of the Internet. We expect to observe that even during 2017.

The IPv6 network graph is not a subset of IPv4, and that needs to be kept in mind. There are ongoing peering wars in the IPv6 area, not between local ISPs, but between those biggest ones. For example, Cogent and Hurricane Electric do not have interoperability, so clients connected only to one of these two networks would never access each other, which is a known issue. Moreover, it is not a technical problem — it is just economics or should we say politics. It has been here for eight years, and it is unclear how many years it would last on.

Attacks bandwidth ratio



All of that kind of issues could easily migrate to IPv4 because the BGP protocol does not require two Tier-1 ISPs to be connected. Clients could force those networks; otherwise, it would not be done.

What this means is that there is a high possibility of that kind of conflict migration from one network to another, from IPv6 to IPv4 and vice-versa.

"IPv6 is entirely another internet, and many do not realize this. Race against the time and competitors in protocol development would again dictate all the breaches and vulnerabilities there would be used when we see more IPv6 connected devices."

However, still there is good news — there still are emergency options, because routes could be different in IPv4/IPv6. Theoretically, we could access those resources by any of those protocols, and multipath TCP would allow that. So it is regular routes reservation on different networks, which could and should be done. It is critical, and it is important. Consider IPv6 as a necessary thing to use and learn, as an investment into the future. IPv6 allows ISPs to drop NAT — a significant advantage since NAT is rather expensive on a high scale — and services interested in availability should be using both IPv4 and IPv6.

DNS, never too good, now horrible

"As a DDoS mitigation company, we often encounter clients hard to deal with. Secrecy, prejudice, and general distrust attitude complicate the process of establishing a healthy business relationship. Often we are contacted in the most critical situations, when everything is already on fire, not for proactive measures. However, we consider overconfidence in one's expertise to be the worst problem on the market.

That can lead to grave consequences as it was demonstrated by Dyn last year. When a specific DNS provider became unavailable, its clients rushed to switch their NS entries. What is the TTL on this operation? A day, more possibly. Regarding availability, a 24-hour delay is tremendous, and anything can happen in that term."

A successful attack on Dyn is interesting as an example of an L7 attack against the DNS protocol, which we have rarely witnessed before. In the past DNS was often attacked with some amplification traffic and that was enough. There are still many vulnerable resolvers, a lot of old NTP servers, and overall, this appears to be a job for a script-kiddie.

When the DNS first appeared in 1987, it was never considered to be a potential attack vector. At the time few believed the Internet would grow in such a manner over the years. Founders of current protocols saw the network like the Internet of trust, and the trust was lost during the period of rapid growth. However, the structural problems remain. The community is highly inertial, and many elements could not be changed.

When DNS is disrupted, all external data center services — not just a single application — are affected.Often under-provisioned DNS infrastructure makes this unique point of total failure a tempting target for attackers.

The industry still uses BIND extensively. **While for HTTP Apache was mostly replaced by Nginx in scalable Web applications, BIND is still here, and it is not considered to be a weak point.** It does not have a substitution of similar prevalence even now, in the world where the large part is a Stack Overflow Driven Development.

In 2017 Qrator Labs expects to see Mirai-like attacks on infrastructure on an upward trend. With the black market where everything is possible if you have bitcoins, few clicks are enough to arrange serious level attacks. Moreover, this is a serious business where the amount of money exchanged is huge.

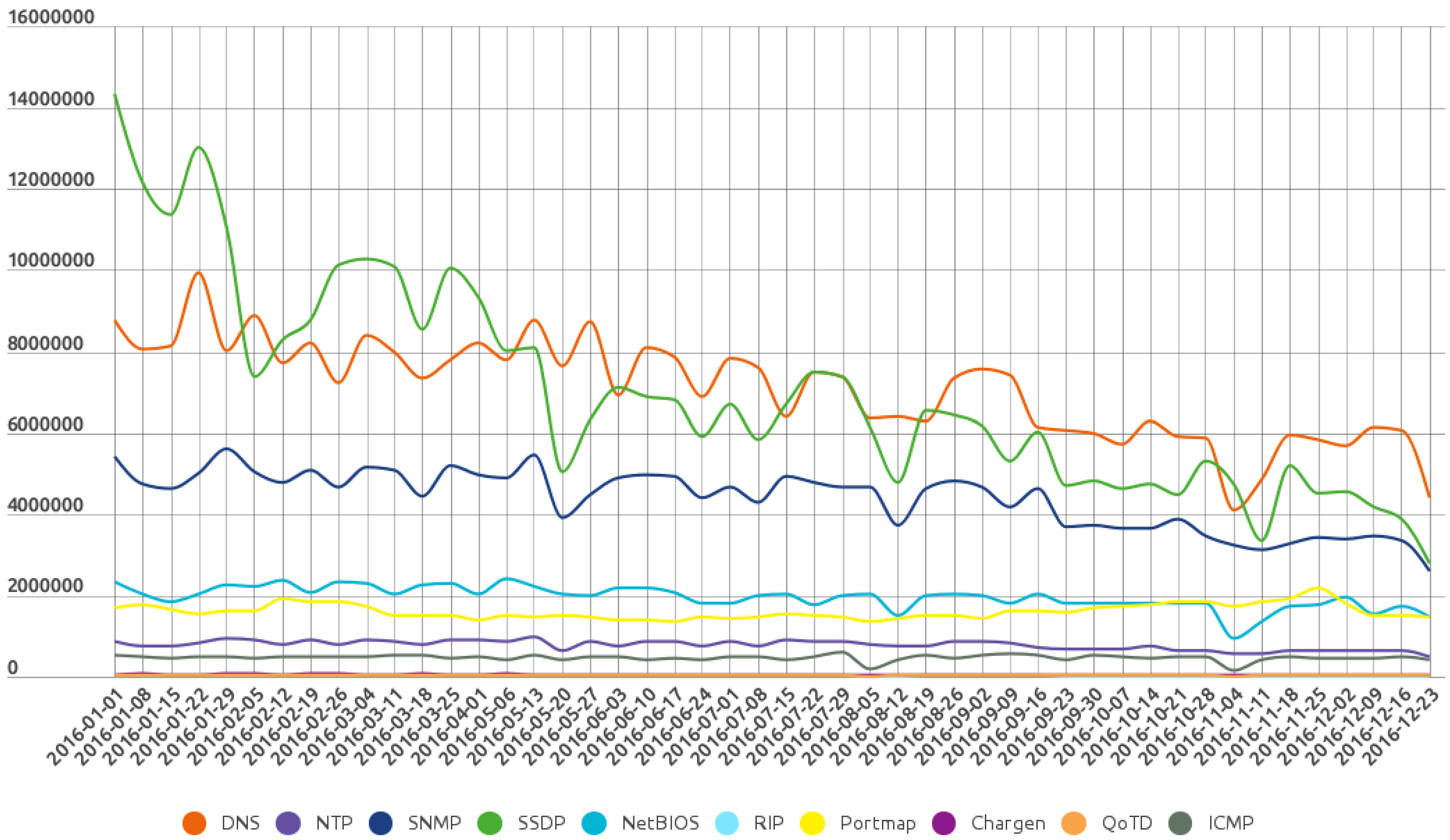
The main problem here is “if it ain't broke, don’t fix it” attitude. “Admin”-”admin” login-password pairs, old software and 0day-vulnerables — all still here, still hurts.

Finally, the TCP - UDP problematics have been here for years. TCP kind of verifies the remote end, UDP does not, so it is faster. That is why all the game platforms are in love with UDP.

UDP is vulnerable to spoofing, where amplification is easy to perform the next step. Quake Network Protocol is an example of an L7 protocol designed in a way that opens the door to amplification attacks. More may come in the nearest future. Before you create any protocol, it is not a bad idea to stop and consider some security scenarios. However, developers often have no forethought to do so.

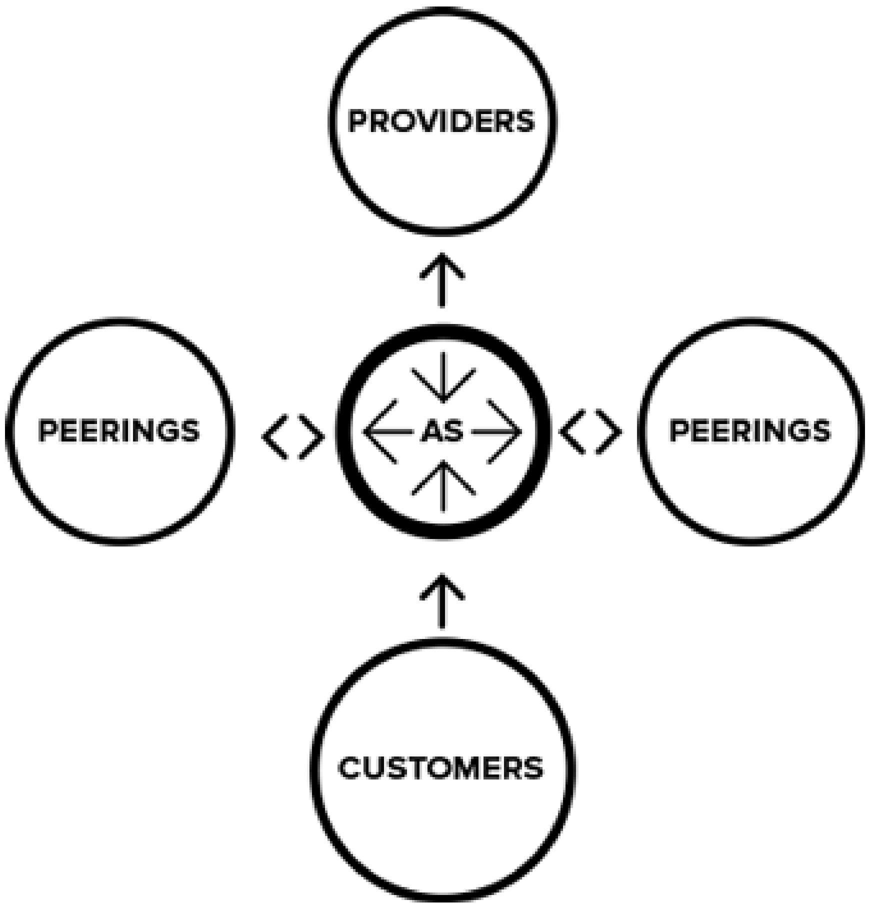
Small DNS servers are over — it is the beginning of a new era

Amplificators count in 2016, absolute quantification



3.2 BGP — a double edged sword

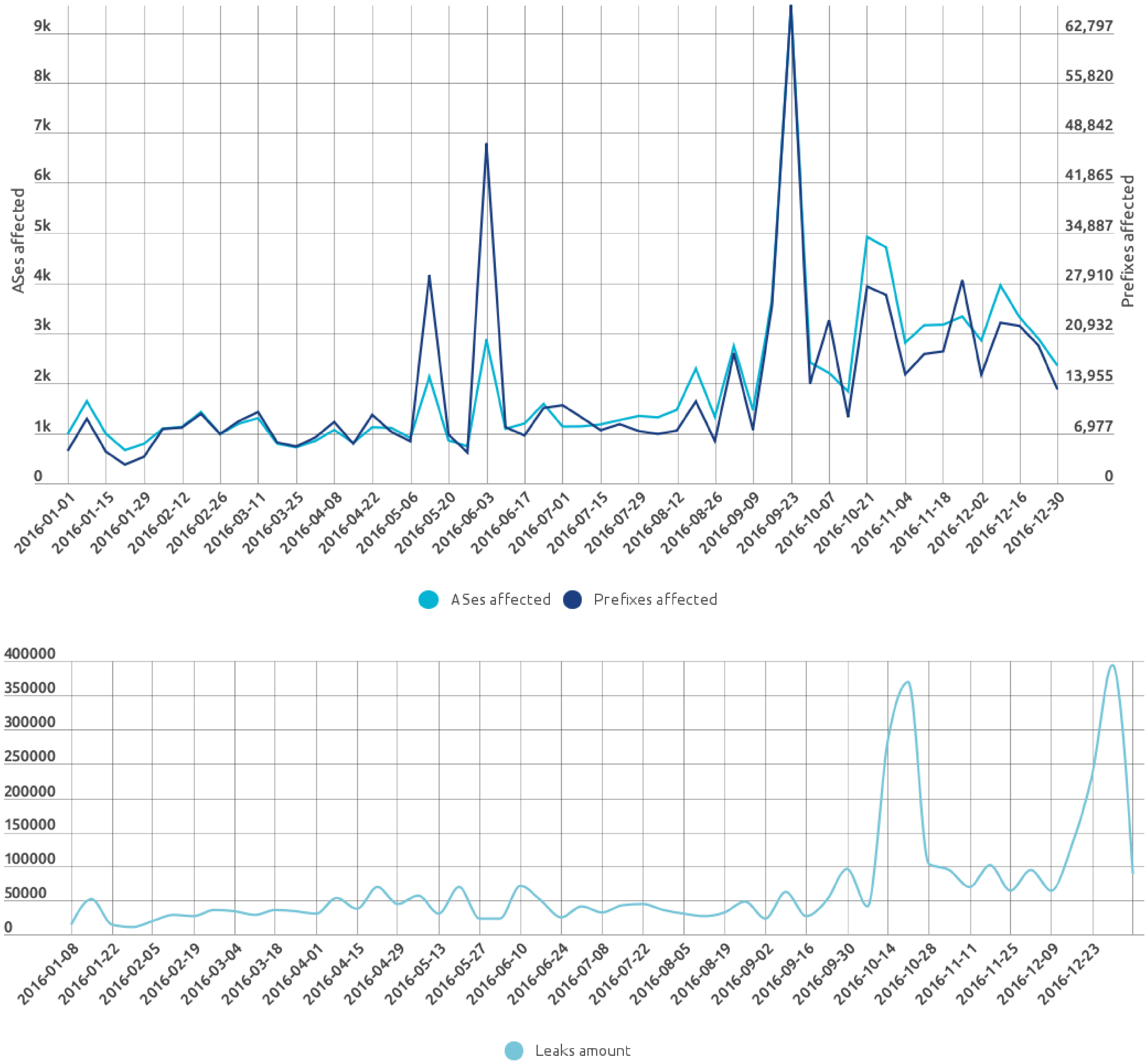
BGP is a protocol modern Internet relies on. It allows route exchange among autonomous systems (AS). Since most of those AS are operated by commercial entities, the protocol is shaped accordingly. BGP is a unique money-vectored protocol, initially built to reflect business relations of Internet service providers (ISPs). So, route propagation around the globe depends on these special business relations.



That means that network engineers have no control over the announcements propagation and the general availability of their network resources all around the globe.

Route leaks as the primary BGP problem

BGP incidents amount in 2016



As we know from BGP design, it accepts advertised routes from other BGP routers by default, which allows not only automatic and decentralized route computation but also accidental or malicious activity. Advertisement in the right direction goes along with the ISPs' business logic, and wrong could lead to traffic routing in totally unexpected ways. Such network anomalies are called route leaks.

We suspect technical specialists who do not fully understand BGP to be in charge for the most of the routes leaking. Here's a default example of how it is done:

Your upstream ISP uses the only list of client's prefixes for outbound filtering. As a result, getting yours prefixes announced from without paying attention to the source of the announce, not only directly from you, it would always advertise them further. That is the point where the problem arises - this upstream degrades, and you try to shut down BGP session with troubled ISP. What happens next? You wait for the problem to be resolved. **However, it is still announcing your prefixes in all directions and getting a significant part of your traffic.**

"This “flexibility” of BGP protocol could also be used for traffic interception, which is a severe issue concerning the BGP protocol, allowing MiTM-style attacks."

A significant percentage of operators are in sin with this, and we are also talking about ISPs at a national level. BGP protocol is not easy to configure, and inbound/outbound route filtering is not automated out of the box. **BGP was created with the assumption that network engineers do understand what they are doing.**

And like many other things with the Internet, BGP was created when the overall amount of AS was counted in dozens. Right now we have more than 50 000 of them. Obviously, some savvy technical specialists could not rise at the same cadence in response to the growing infrastructure.

There is an enormous ambivalence: **to correctly tune the BGP protocol you have to know a lot, on the other hand - to make it "just work", very little**. Common practice is to copy and paste examples from Google search results. Lack of expertise is why there is a huge amount of route leaks. There is high potential for destruction and no “driving exams,” no penalties. This could not be ignored anymore, especially after Malaysia Telecom leaked in such a style that several biggest ISPs were out of service.

Separate AS incorrect setup could lead to other ASes abnormal activity and behavior

IETF is the place

We do not conceal the fact that we entered the IETF negotiations with a self-centered idea — anycast-networks are highly vulnerable to route leak incidents.

At first, we just wanted to know when prefixes are leaked and who’s in charge. Since the reason for most leaks is an incorrect setup, we understood that the only way to solve this is to eliminate those environments where engineers copy and paste something wrong. To make BGP’s optional mechanism a default one, and to lower the level of complexity of tuning the BGP protocol.

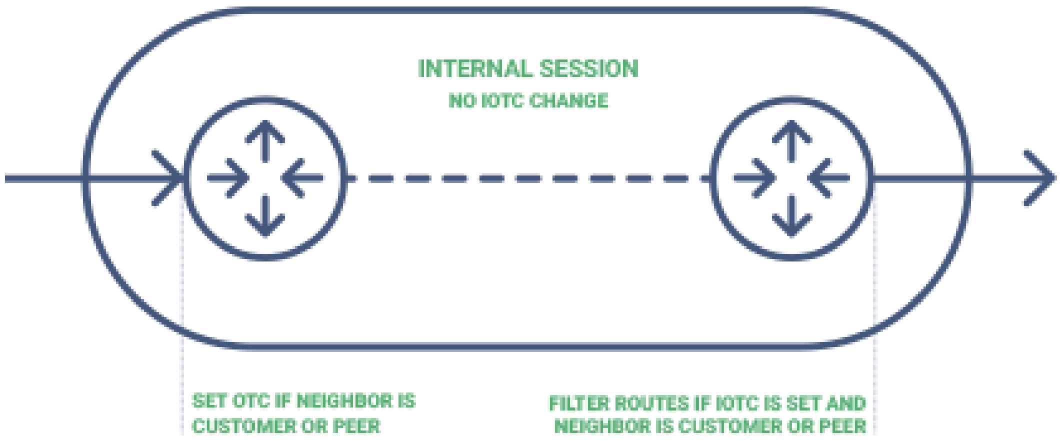
Of course, this process would take years. However, we try to make the “new BGP” not only “safe” in the sense of “route leaks cannot appear.” In case a route leak happens in the stage of partial deployment this BGP extension would also provide a mechanism to detect route leak and stop its propagation automatically.

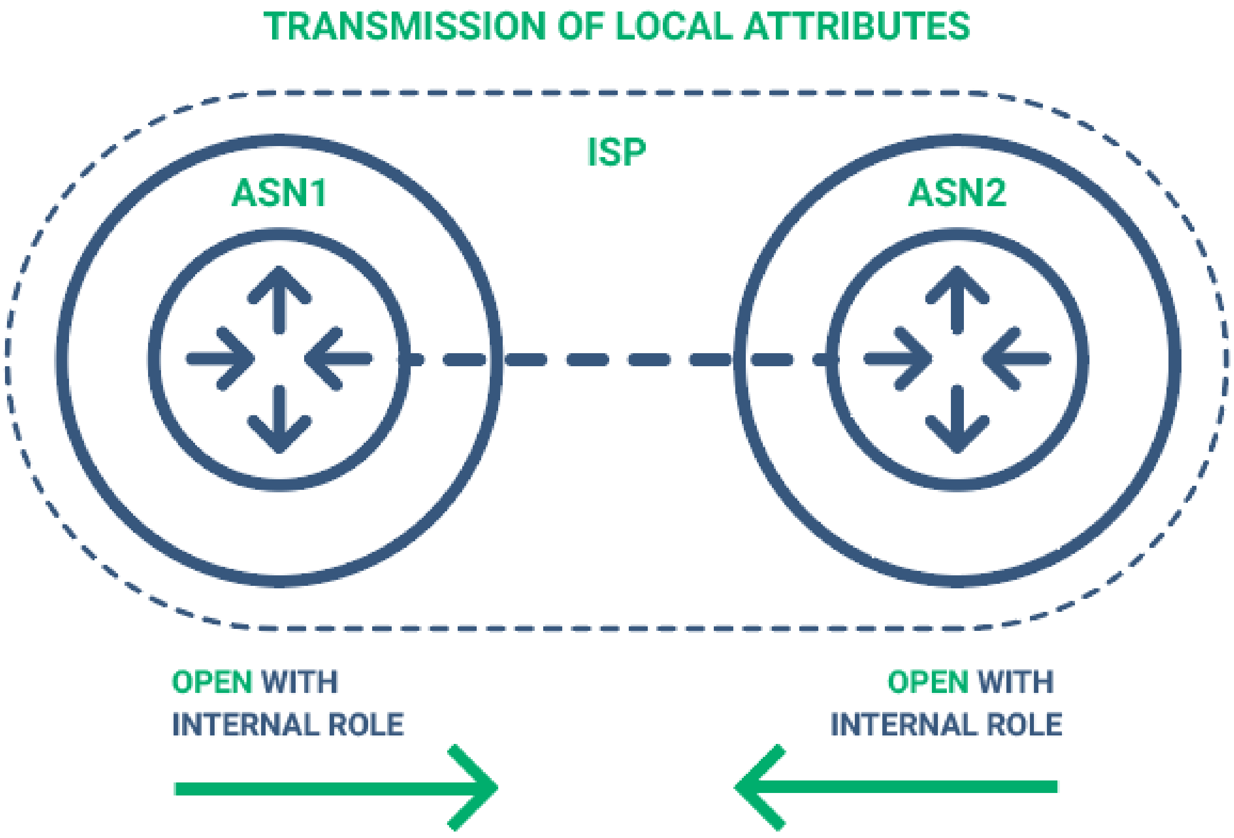
"The Internet Engineering Task Force (IETF) develops and promotes voluntary Internet standards, in particular, the standard and extensions of BGP protocol. It is an open standards organization, with no formal membership or membership requirements. All participants and managers are volunteers, though their work is usually funded by their employers or sponsors. Since 1993 it operates under the Internet Society, an international membership-based non-profit organization (Wikipedia)

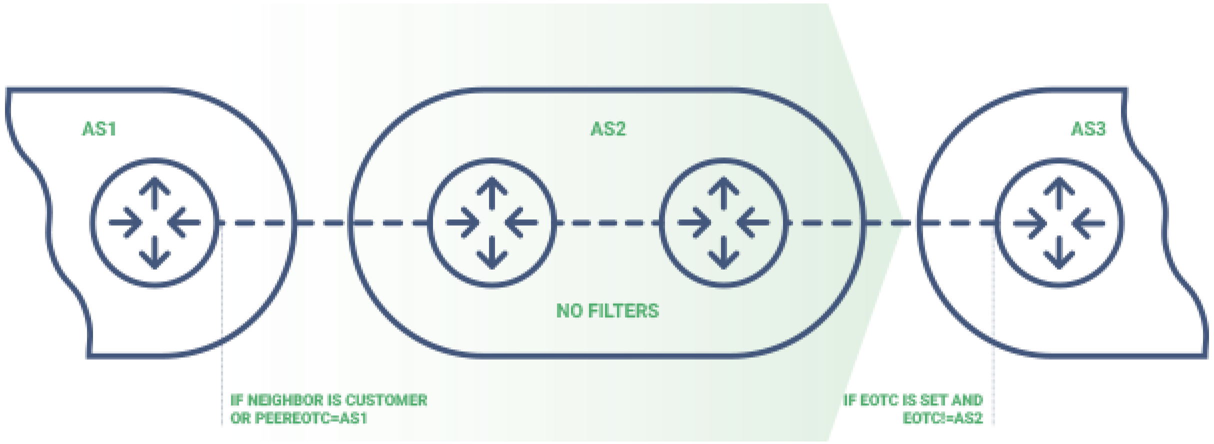
IETF isn’t a legal entity, it is only a community, which allows it to be independent of any legal issues and regulation laws of any country, which is generally, smart. Something that does r exist in physical form can not be hacke attacked, or sued. IETF does not pay salaries, which means that everyone participating does it by volunteering to task force. This also means that this act hardly goes on a priority higher than a ‘ profitable” one. So the process of proto design is often slow. The only exceptior the IETF conferences, which are an acti epicenter.

But where things get tough is at a working groups, which have its specific areas of responsibility. When the consensus on general subject within a working group is reached, it starts to work on the first versions with initiators — authors of the proposal. When the working group considers the work done, the draft goes to area directors — their primary goal is to double check everything. Afterward, IESG provides the final technical review. The document then forwarded to the IANA since it makes the needed reservation for any protocol changes."

If the draft with a new BGP extension would pass all the hell circles and would be accepted, route leaks would just dry up, and they would not be such a severe issue anymore. Of course, malicious leaks would still be here but would be handled in a different way — with persistence monitoring.


INTERNAL SESSION
NO IOTC CHANGE
SET OTC IF NEIGHBOR IS CUSTOMER OR PEER
FILTER ROUTES IF IOTC IS SET AND NEIGHBOR IS CUSTOMER OR PEER




AS1
AS2
AS3
NO FILTERS
IF NEIGHBOR IS CUSTOMER OR PEEREOTC=AS1
IF EOTC IS SET AND EOTC!=AS2

Illustrations from the IETF draft. More at https://radar.qrator.net/tools/route-leak-mitigation

MOAS conflicts

MOAS stands for "**multiple origin AS**," which means identical or overlapping prefixes originated from different autonomous systems. MOAS repeatedly occur as result of malicious activity - in this case, it is called hijacks, but not necessarily a MOAS conflict would be illegal. Sometimes we know this to be the possible solution to specific networking cases. For example, Amazon could announce their address blocks from different autonomous systems in the various regions, and it is OK in this cloud. However, of course, this could be misused by criminals when hijacking some address space for further deep packet inspection (DPI).

Today, the most common case is when a malefactor steals only a part of huge address pool, which goes unnoticed by an ISP (if there are no working services, for example), and then starts using it in cyber-attacks, spam distribution. When this gets traced, criminals just switch to available address pool that belongs to different ISP and continues their "work."

Before 2016 this problem was hushed up, most ISPs did not treat this seriously. This year marked the rise of attention towards the MOAS issue, which could be tied with the IPv4 pool exhaustion and potential reputation losses for hijacked ISPs. There are organizations like Spamhaus, which could easily list you in a publicly available list of spammers, and it is very hard to prove afterward that you are innocent.

In case crooks would misuse those hijacked addresses, due to the IPv4 pool exhaustion, this could become a serious issue for some companies and their clients. This issue is very actual, even though we did not receive such public attention as for hijack of YouTube in 2008 or massive hijack by China Telecom in 2010.

154,955 MOAS conflicts at 2016

More hijacks for more reasons

"Roskomnadzor is a Russian federal executive body responsible for control and supervision in the field of media, including electronic media and mass communications, information technology and communications functions control and supervision over the compliance of personal data processing requirements of the legislation of the Russian Federation in the field of personal data, and the role of co-ordinating the activities of radio frequency service. It is also the body administering Russian Internet censorship filters."

> ISPs have to obey laws — in some countries, regulators limit or restrict access to specific resources

The situation leading to the hijack could be of a legislative origin. For example, in Russia the regulator (Roskomnadzor) wants some IP addresses to be blocked for all internet users within the country. Some ISPs, instead of correctly configuring their hardware and software for this kind of filtration, just ask higher tiered ISP to “help on this one.” Then higher ISP hijacks target set of IPs and announces this pool to its customer. That leads to the following consequences:

— **ISPs serving this kind of “service” when asked often forget to add a no-export community**, which results in unguided propagation of those hijacked prefixes. As a result, a service restricted in one country could become globally unavailable.
— Often we see not a /32, but a much larger /24 prefix hijacked. This mistake is so serious that it could theoretically produce a global outage. The whole IP network hosting the restricted resource, which is often a large hosting provider or a CDN, can go down for hours or even days before the issue would get resolved.

With current BGP protocol, when one sets up an announcement improperly or violates best current practices, there is always a possibility that the wrong announcement would propagate globally. Those issues are hardly findable when you seek for the problem source only within changes in the traffic pattern of your autonomous system.

Bogon ASNs

194,327

2016 amount of prefixes with a private AS at the ASPath

30%

What percentage of the global routing table this amount represents

For years, bogon ASNs were not seen as such a big issue. Most often, within the ASPath attribute (reflecting the ISPs consequence with an endpoint of the prefix announcing AS) we observe private AS numbers, which clearly contradicts RFC 6996.

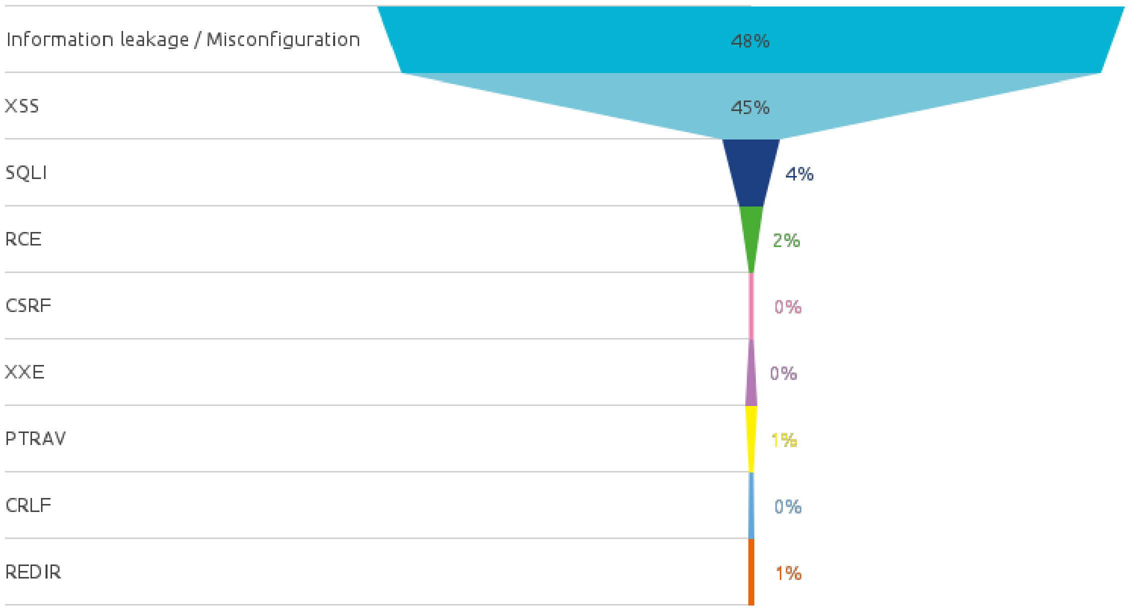
In 2016 several big ISPs declared that the issue with bogon ASNs is something they are paying attention to, and going on a crusade against. They asserted that they would filter all bogon routes. The example was managed by NTT (AS2914), one of the Tier-1 ISPs.

So, if any ISP adds private ASN to paths of announced routes, it’d just become inaccessible globally. The problem is that its clients would also be affected and as a result could experience unpredictable traffic changes, service degradation, and even DoS. This mechanism could be easily used to create artificial network anomaly for target prefix with mentioned results, but right now we see bogons as mistakes in BGP configurations.

3.3 Application level issues

Vulnerabilities distribution in 2016

XSS and Misconfiguration Run the Show



> *"A pandemic of attacks on many different services began with malefactors making quick tests of logins and passwords they had in these databases. The widespread practice of reusing the same password for social networks, e-commerce marketplaces, and every other website results in an incredible efficiency of these attacks. Malefactors obtain thousands and tens of thousands active user accounts on services which were not hacked. This year we observed widespread problems among online retailers, payment systems, travel websites, and many other segments."*

Most severe software vulnerabilities

Credential stuffing attack epidemy started in 2015 but became even more widespread occurrence in 2016. Staggering by their scale user database leaks of several companies, including the biggest Internet websites, led to the fact that malefactors obtained consolidated login-databases (which often are e-mails) and passwords of millions of people. Users' accounts on any other service on the Internet were endangered as a result.

Malefactors use huge botnets for high-frequency attacks. These botnets are hard to block even using special-purpose security tools. This type of attacks can be noticed by an abnormally high load on the system. CAPTCHA deployment allows to complicate the task for malefactors, but attack quickly switches to API (e.g., for mobile apps), where robot screening is much harder to implement.

One of the biggest retailers of electronics suffered from credential stuffing during 2016. A Russian e-payment system, and a bank, also was a target for criminals trying to obtain users' accounts. In 2015 one of the ISPs lost his user's database with logins, passwords, e-mails, phone numbers. Since then we have observed many attacks on different payment systems and Internet banks using credentials related to that data bank. Of course, we cannot forget the LinkedIn, Ashley Madison, and Yahoo incidents - they still echo.

"In 2016 we also saw an unyielding trend on shortening of time periods between proof-of-concept for vulnerability and further exploitation of it. Nowadays the term is somewhere between 2 and 4 hours depending on the breach, but in general, we see a 3-hour window between a report on the vulnerability and first attacks. That is something quite serious. It shows us that criminals are getting more and more prepared, professional, and they are working much faster. In 2013 we considered a week as a mediocre timeline between the report and actual hacks, so there's been significant progress on that."

No time to patch

Hacking timeline shortening at the Joomla RCE example

Less than 24 hours

Less than a day is needed for criminals to find a hacking option after patch release

36 hours at max

Timeline between new breach-containing patch and mass vulnerability exploitation

x0000 hacked servers

Within 36 hours after first scans

That is crucial considering the period needed for patching is not that short. How quickly can you patch a serious breach? Depends on how serious it is — maybe a day, maybe a week. In 2017 there would be even less time to react to hacks and attacks. We expect this period to shrink down to 2 hours in the nearest future.

How does one protect their systems that fast? **Only by proactive monitoring, says Wallarm CEO, Ivan Novikov.** Our aim here is to block attacks preventively in real-time when we see them. Moreover, the second important factor is to search for those vulnerabilities and security issues proactively. Without a system like that there is no reason to be 100% sure about the safety of your business.

Attacks are already automated, and this is the main reason why manual defense is not a viable solution these days

"At Joomla (RCE vulnerability) we observed a 24-hour period between releasing patch notes and first exploitation attempts and a 36-hour between patch notes release and mass use of the vulnerability. The entire IPv4 address pool can be scanned in 5-10 minutes today, for domain pool, this is possible in hours. Because of that in short period after it is clear that there is vulnerability most malefactors already may have lists of Joomla and Wordpress websites that can and will be attacked. So criminals are very targetive these days especially when it comes to free and open source products installed by the user."

IoT: where “T” stands for “Threat.”

The “Internet of Things” phenomenon is also something that causes concerns. **Before 2016, we at Wallarm tested several devices from big vendors and came to a very disappointing conclusion: almost every device, even from most major brands, was vulnerable.** At that time we approximated this on the worldwide level. It was clear that in a short period there are going to be some far-reaching problems with IoT.

In 2016 our predictions came with full strength with Mirai and other IoT-related botnets, which exploited devices with default logins and passwords and visible to all the outer world — IP-cameras for example. After you logged into, let’s say, a camera, you have an option to refresh the device or find a breach in code execution (injections are also an effective option here). That can be handled on the network level. **It should be mentioned that every type of hardware is exploitable, it does not narrow down only to IP-cameras, routers, and DVRs.**

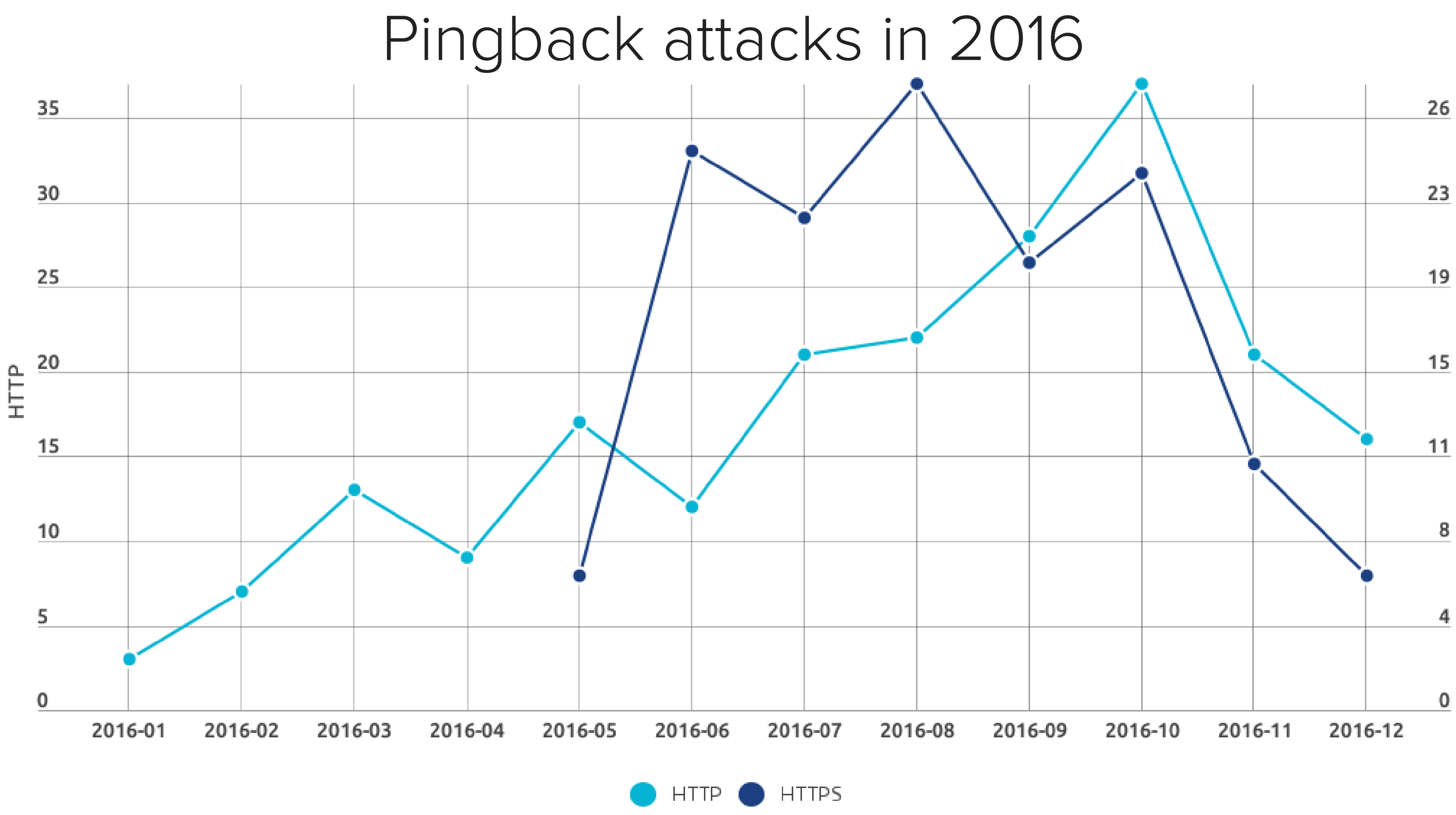
Trendy technologies reason and understanding

Another important part of the defense landscape is that companies tend to integrate corporate (local) clouds for their needs, but they severely lack security techniques and defense practice. **The technological stack is growing rapidly, and soon there would be programming areas where no code has to be written to make something work.**

New tools and instruments are frequently released, but no questions are raised about security and potential breaches. **If it works, if it simplifies the developer’s work — it is being used in production. This attitude is another serious problem.**

The tendency of simplifying the entry to IT development, in general, amplifies the issue. The technology stack gets more and more complicated for people who enter the programming area quickly.

Wordpress — a potential attack vector

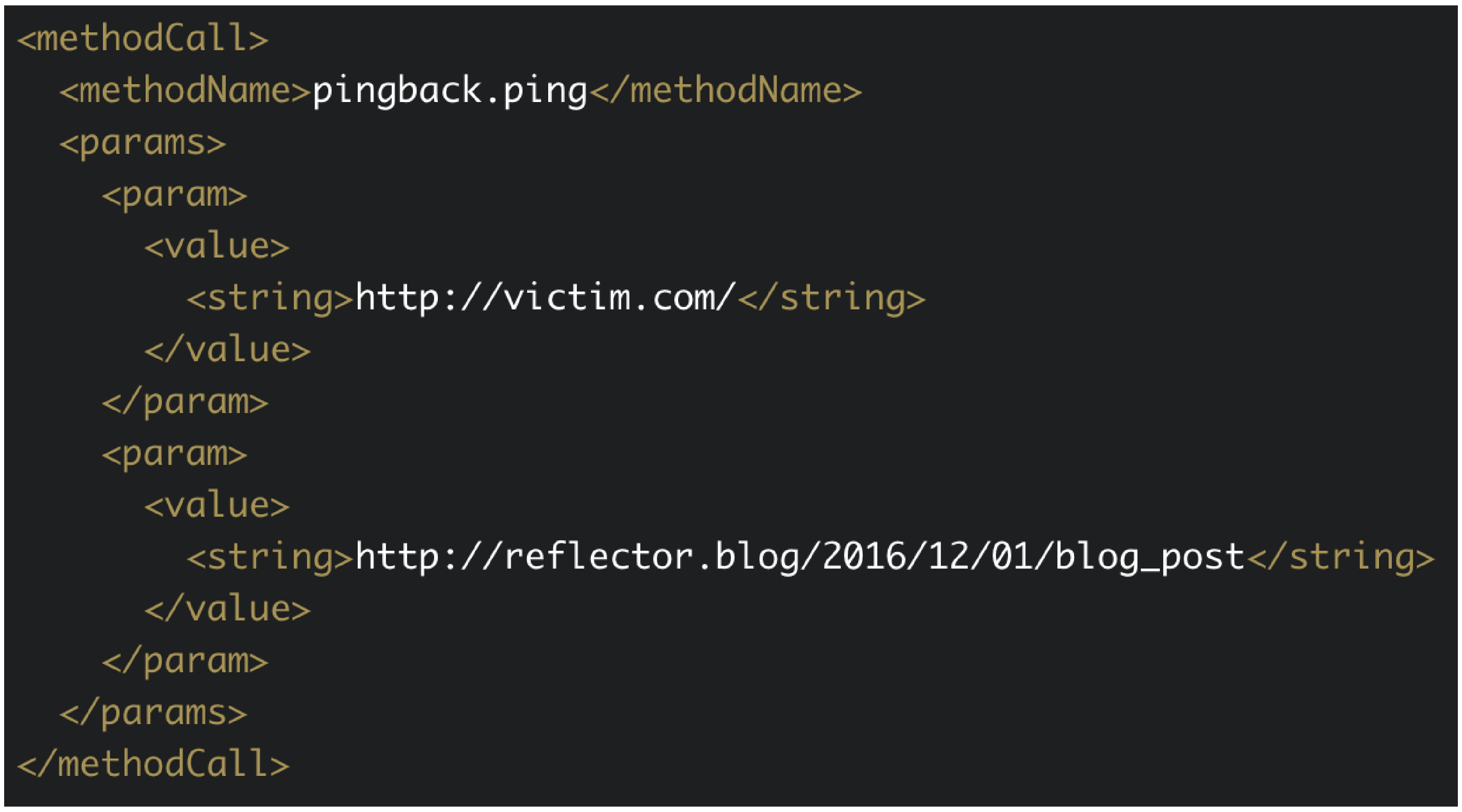


WordPress CMS was created as a ubiquitous and functional engine for blogs. Among other features, it had Pingback which is a small piece of functionality allowing standalone blogs to exchange information about comments and mentions — a very useful feature by the way.

The security problem here is that this function is turned on by default and implemented in such a way that a malefactor can, by forging a specific XML-query towards a vulnerable Wordpress server, a force that server to retrieve an arbitrary Web page anywhere on the Internet.

That could be (and is) used for masking original IP-addresses of a botnet, while regular HTTP flood may reveal it. This technique is used as some kind of amplification attack. **This attack is called WordPress Pingback DDoS.**

That is how a custom XML query for the attacked server could look like9



```
<methodCall>
  <methodName>pingback.ping</methodName>
  <params>
    <param>
      <value>
        <string>http://victim.com/</string>
      </value>
    </param>
    <param>
      <value>
        <string>http://reflector.blog/2016/12/01/blog_post</string>
      </value>
    </param>
  </params>
</methodCall>
```

"It is interesting that a Pingback attack towards HTTPS, while fully encrypted, is not complicated at all — the attacker just has to replace “http” with “https.” If a resource is available using HTTPS (a bank or some other service related to finance), it could get this vector exploited. We registered first attacks of those types (both HTTP and HTTPS) in 2015, and it is still a working vector."

Mitigation of encrypted attacks is more difficult, but Pingback DDoS leveled these problematics even higher. Since we have millions of vulnerable Wordpress servers, hundreds of thousands of those could be used in one attack, each having a rather good connection and server performance.

Therefore to mitigate these attacks successfully an Internet connection with a capacity of 20 Gbps or higher and ability to handle L7 wirespeed are required. Besides one, has to decipher all TLS-connections in real-time and on the go, which is a complex task. ISP-based solutions were simply unable to do that without additional tuning on the mitigating device and the customer’s server itself.

Concerning everything above, from the beginning of 2016 with free Let’s Encrypt SSL certificates and mass HTTPS adoption we saw those attacks rise in amount and power. 28,98% of all Pingback-based attacks during 2016 were performed using HTTPS protocol.

"This Wordpress vulnerability differs from the Joomla one is because RCE affects the vulnerable service itself, while Wordpress Pingback is not noticeable to its users. A server could be actively participating in orchestrated attacks while working as usual and being available for legitimate visitors. That was the reason why Joomla was actively patching those breaches, and Wordpress still has issues, allowing misdoers to exploit millions of Wordpress services."

The HTTPS attacks also buried most popular ISP defense products. **While with L7 there are at least some tools to track traffic (headers, masks), with TLS you have to obtain an encryption key to decrypt data sent by every service for each and every of your clients in real-time**. Also, the customer has to follow certain rules, for example, some specific encryption protocols need to be disabled. Otherwise, even with the private key, nothing can be done.

CAPTCHA is not effective anymore
(and we are telling that for a long time)

Results of the CAPTCHA solving competition among students

40% out of 10,000

Efficiency of the winner's automated CAPTCHA solver solution among student visitors at the ZeroNights conference

5 * 2000

5 different types of CAPTCHA in Klingon were used (one type was excluded by the winner)

"At ZeroNights 2016 we held an event where we showed how a student in a day designed an algorithm capable of passing CAPTCHA test with 40% efficiency.

ZeroNights anti-CAPTCHA competition demonstrated how a solution, previously considered as a straightforward and trivial, stopped working in 2016."

Most vendors still think that “browser = human,” which 2016 demonstrated to be false. In the last four years, we noticed full browser stack-enabled botnets based on computers with Windows, which do have real browser capabilities like mouse movements tracking, Javascript interpreters and so on. Old methods like CAPTCHA and browser capability test do not work.

Every ad network (including Google’s) has its anti-fraud system. As Methbot fraudulent bot farm demonstrated, these systems may be vulnerable as well.

In Soviet Russia robots solve CAPTCHA better than humans.

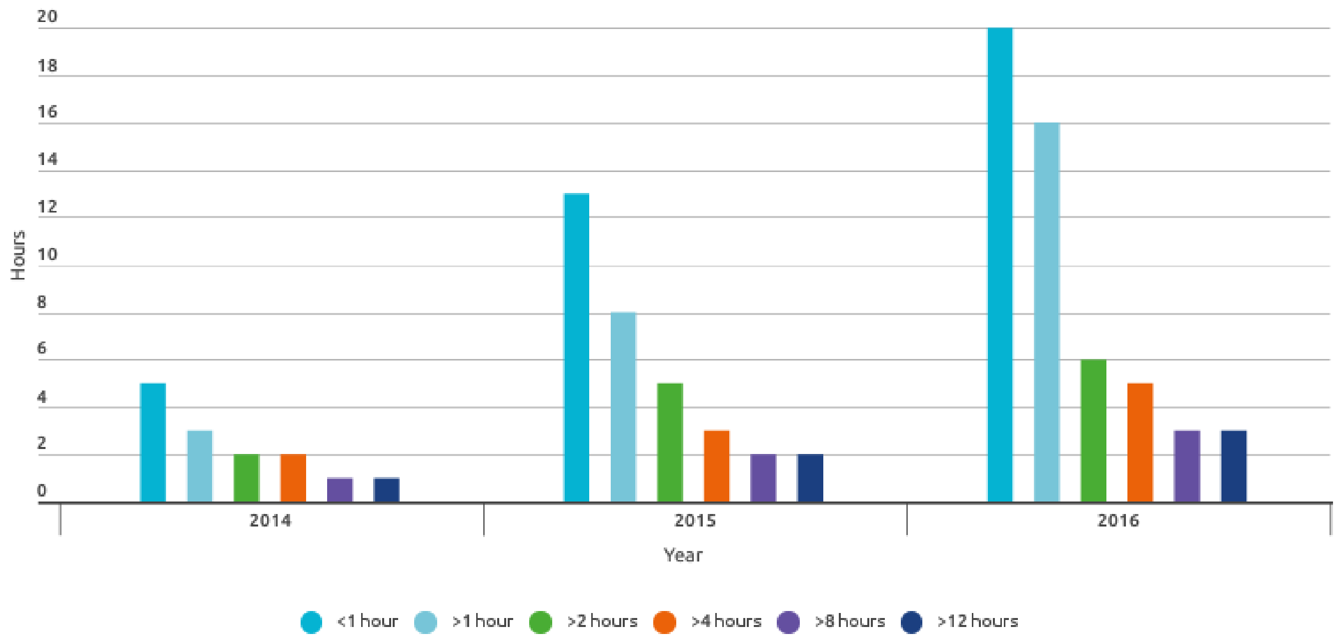
Next: 2016 Conclusion

Conclusions on 2016

"We witnessed landscape shifts in 2016 when most companies and clients realized that in worst cases operator-based solutions failed to help make services available again. Of course, the infrastructure is crucial, but rigid and highly regulated industry rules, compliance with strict norms will not secure the business on their own — it is just something that buys confidence, not actual safety."

Hit and Run strategy works

Average attack duration, hours



Top-level findings

In general, there are three types of attack mitigation solutions:

— **Dedicated CPE with a crew.** The most expensive and hard-to-build and use option, but the most preferable by the biggest companies since traffic, keys and everything else are locked in one infrastructure under one control and management. Licensing from PCI DSS to USdot is available with this style of defense.

— **Distributed or "cloud" solutions**, an external resource and a network, where traffic is filtered and managed. In this case, with a decent service provider, you do not need your staff to maintain this perimeter, you do not need huge uplinks. However, the drawback is that you have to give away some of your data to the third party, and not every company could agree to that.

— **Hybrid solutions**, generally either splitting L2 and L7-level attacks (with the former ones mitigated in a cloud and the latter ones dealt with at the customer premises equipment) or handling all the attacks at a CPE except for the cases when an attack floods up all the client's bandwidth, in which case the traffic gets re-routed to the cloud.

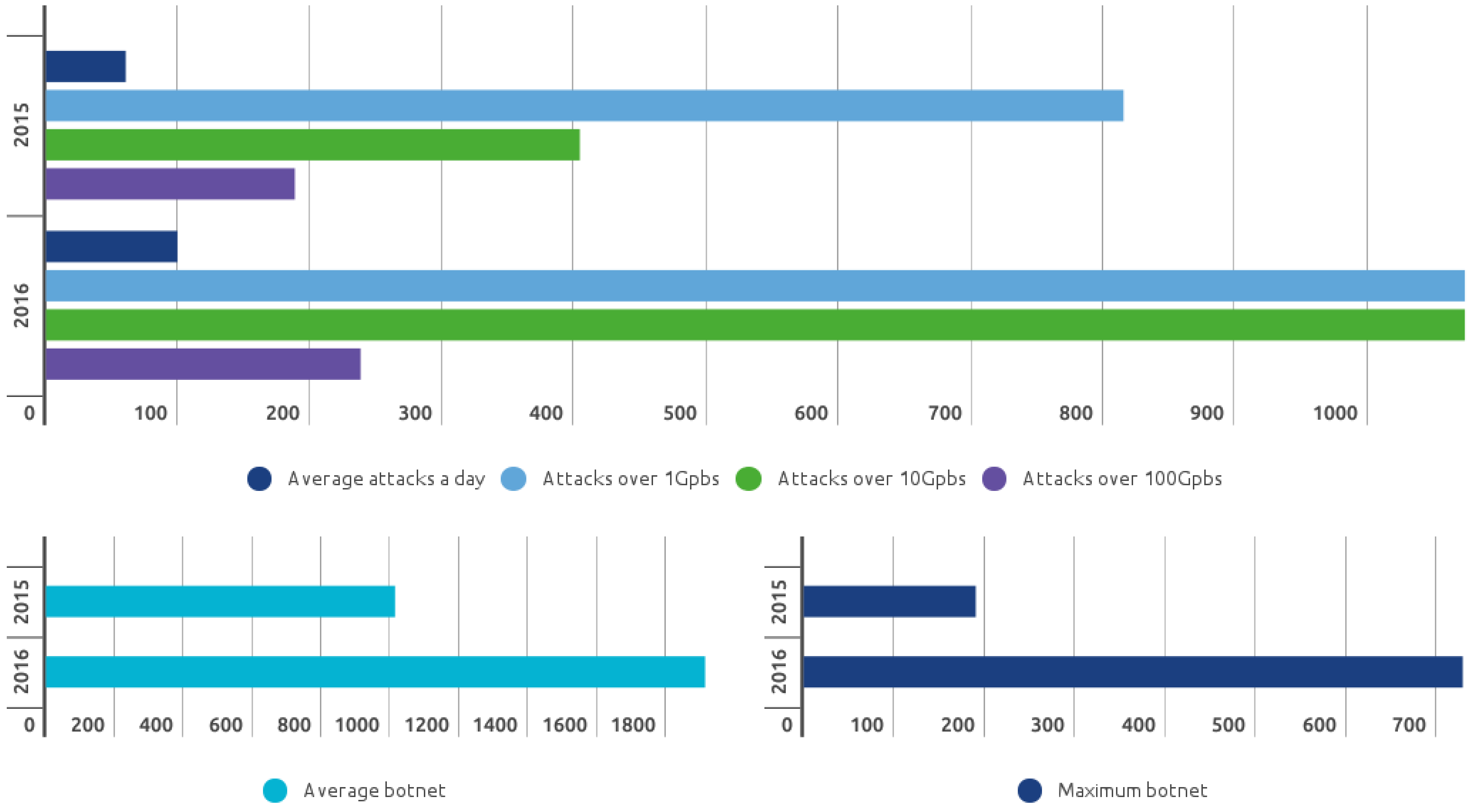
"With Wordpress Pingback and especially Mirai attacks we saw that even a full crypto-enabled attack at L7 could utilize 20 Gbps of bandwidth. The only way to survive such attacks is not only to build TLS-capable and session-capable DPI but also to utilize behavioral and correlational analysis in your systems. All of this at very high speeds getting close to 1 Tbps in 2017."

> Few individual companies can survive
> attacks we witnessed recently

The first kind of solution we listed had a poor-performing period in 2011-2012 when 100 Gbps attacks became a reality. CPE vendors could not affirmatively tell their customers how they are going to handle those type of attacks, at that time new and powerful.

That was the time when the “hybrid solution” was born. Moreover, it satisfied many companies for almost 5 years: there is some hardware that you have to update, but it is still at your site, under control of your technical team. Only in the case, that attack rate is higher than the one stated by the manufacturer your traffic is forwarded to the cloud for filtering. However, with recent attacks, even hybrid solutions perform worse and worse.

Attacks specifications at 2015 - 2016



> *"Moreover, what we expect is that within 3 years that new and more powerful kind of attacks would become an industry standard, just like now you cannot surprise anyone with a 100 Gbps one."*

Russian banking landscape

The chain is as strong as is its weakest link, and with Russian banks it’s the first time every time

100% of surveyed technical and infrastructure specialists at banks claimed that they have security perimeter under control and close watch.

80% of businesses do a security audit on a yearly basis, while only

61% percent of surveyed companies were cautious because of risks of banking license revocation (PCI DSS).

55% percent of the companies experienced false positive cases of software reaction to incoming traffic and ongoing attacks.

24% of companies responded that DDoS was number one threat they face, **while 69%** still used operator-grade DDoS mitigation solutions.

Only 19% of them tell that any issues are found during the audition.

Peculiar is that **54%** of more than hundred banks and e-payment systems supposed that their traffic was not sent anywhere for analysis. Which is almost always wrong.

> *"On a theoretical level, Russian banks were ready. June 1 a FinCERT center was established, too late for mitigation because mainly clients were under attacks, not the banks’ infrastructure nor their services directly. However, in 2016 they had to meet villains in person. According to the FinCERT statistics, from Q4 2015 till Q1 2016 no less than 19 major incidents with 2 billion roubles total losses happened. The level of threat was evident enough to double the FinCERT staff, but we still have no understanding whether banks started to believe in this danger."*

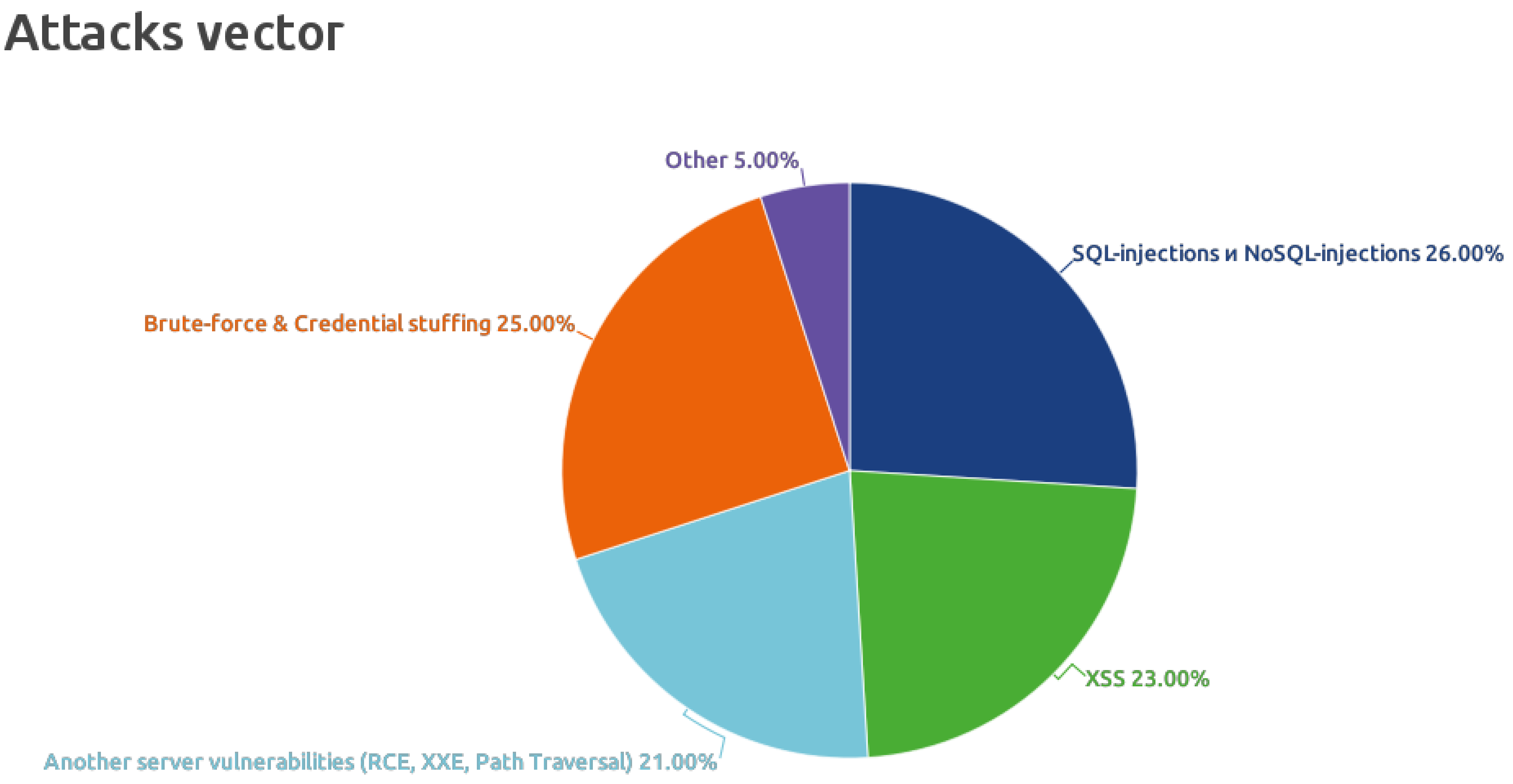
Banks have always been in the comfort zone, because even during attacks they always survived, hadn’t lost much and continued to operate. Lack of awareness and expertise in the field is so high that lack of attacks — not actually mitigated attacks — is often considered a good performance for the anti-DDoS software and hardware used. **Some customers may switch to another mitigation product, encounter their first attack, and consider the new product to be worse-performing.**

The Central Bank of Russia and law enforcements are now looking at the problem closer. Banks have to pay attention: there would be more audits and license revocations in case there would be severe information security flaws and no attack mitigation set up and ready. We consider this process as efficient because this is the area where the market is probably weak and should be motivated by the regulatory organizations.

In Russia, during 2016, there was an ongoing media hype on this topic. **It is hard to predict what banks could be next targets and how severe would be the damage.**

Hacking in 2016

Application layer yearly attacks distribution



"Nobody is immune to hacks, small company or big — everyone is vulnerable. Dropbox, LinkedIn, Ashley Madison — the list of known victims goes on, while sometimes the information about the breach is not even disclosed. However, there's also a brighter side: plenty of public attention was brought to the information areas that were appealing only to specific professionals. More and more people begin to care and think about their network and application security."

Agile, continuous integration and delivery make companies work and market in a much faster cadence they did before. **Ten years ago an average bank could upgrade its application once a month**, now it is at least once a week, the best and most secure banks we see on the market perform even daily updates. That means that companies need new tools, new professionals to make it work in the same efficient manner they did before.

To defend proactively and to integrate information security techniques into development process companies now have to keep their DevSecOps guys ready and available. Nowadays all system administrators, DevOps staff, and other developers responsible for the crucial parts of applications have to know defense practices to be certain about the security of their product in dangerous situations which would happen as we illustrated earlier.

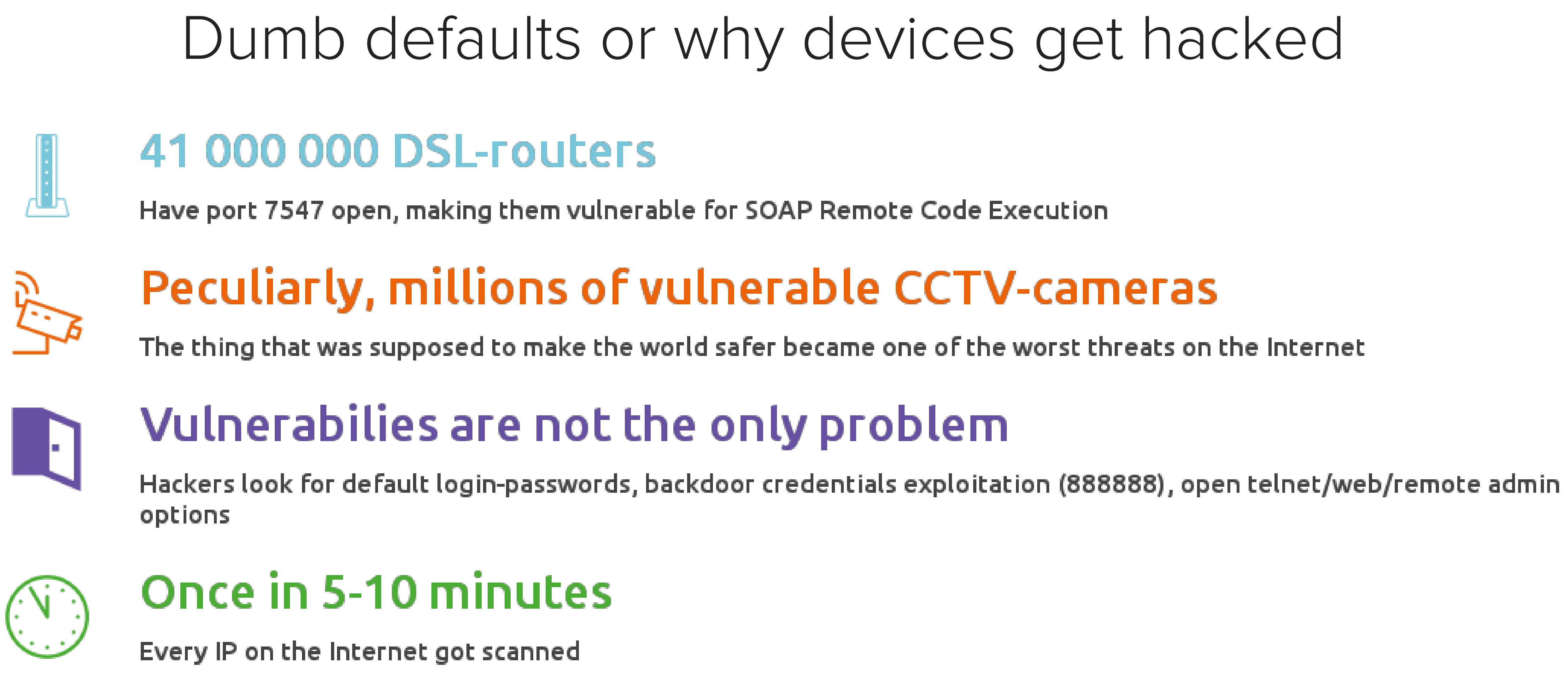
L7 application layer attacks

The general theory is that the higher layer attack we have, the more resources we need to mitigate it, but we still have some myths out there:

- Application layer attacks are simple (**“I built it, I know how it works, I can filter anything”**);

- “I can understand when it is an application, or network, or transport layer attack” (**“I do not know the basics, but do I need them?”**).

Major hacking vulnerabilities



Dumb defaults or why devices get hacked

41 000 000 DSL-routers

Have port 7547 open, making them vulnerable for SOAP Remote Code Execution

Peculiarly, millions of vulnerable CCTV-cameras

The thing that was supposed to make the world safer became one of the worst threats on the Internet

Vulnerabilies are not the only problem

Hackers look for default login-passwords, backdoor credentials exploitation (888888), open telnet/web/remote admin options

Once in 5-10 minutes

Every IP on the Internet got scanned

1. Usage of **outdated software** and lack of means to quickly patch it after vendor issues an update: e.g. Wordpress and some of its plugins.

2. Unprotected minor resources on network perimeter of the project, which were abandoned and forgot about.

3. Trivial critical vulnerabilities added on software development or modification stages.

4. System management issues: default login-passwords pairs, reckless copying of setup scripts from question and answers websites.

5. Target attacks on employees with the required level of access (passwords/keys for FTP, SSH, VPN) are done using phishing.

6. An accidental leak of authentication data to open web: code exchange on developer web forums, pastebins, access keys left in GitHub repositories, etc.

The IoT malware went by several names, including **"Bashlite," "Gafgyt," "Qbot," "Remaiten," and "Torlus."**

All of these related botnet varieties infect new systems in a fashion similar to other well-known Internet worms — propagating from one infected host to another.

And like those earlier Internet worms, sometimes the Internet scanning these systems perform to identify other candidates for inclusion into the botnet is **so aggressive that it constitutes an unintended DDoS on the very home routers, Web cameras and DVRs** that the bot code is trying to subvert and recruit into the botnet.

This kind of self-defeating behavior will be familiar to those who recall the original Morris Worm, NIMDA, CODE RED, Welchia, Blaster and SQL Slammer disruptions of 2016.

There would be more and more victims and
compromised devices over time

Now when 900 thousand users could instantly go offline, Sony cameras have backdoors, and the news on new security breaches over all kinds of software **does not even surprise**.

The situation is more serious than it appears to be. At first passwords were bruteforced, then security breaches and backdoors were used, now malefactors reverse-engineer the newest firmware and know right away, where exactly the breach is on a device.

The severity of situation increases since it is still quite complicated to update such firmware. It has to be done manually, with special tools, backups and everything else — it is often long and complex task even for qualified technicians.

"MongoDB databases decimated in soaring ransomware attacks at the beginning of 2017:

1. Internet Scan
2. MongoDB/Elasticsearch default settings servers search
3. Access, data encription
4. Extortion"

Most severe software vulnerabilities in 2016

Wallarm statistics on the number of malicious requests blocked and vulnerabilities detected

2,400,000,000
Malicious or suspicious requests detected

33,182
Vulnerabilities discovered

DirtyCow
Privilege escalation
Allows escalating privileges on most of the versions of Linux kernel as well as operational systems based on it (including Android). Linux is often deployed not only on web-servers but also on many Internet of Things devices: routers, smartphones, smart multicookers, and TVs, etc. An attacker with local access to CLI may use this vulnerability to gain root privileges. A successful exploit may allow to leave guest Docker container and obtain access to the host OS.

imagetragick (CVE-2016–3714)
Critical vulnerability in ImageMagick, popular software suite for image processing used throughout the web. Researchers published a report on multiple vulnerabilities, and one of them allowed arbitrary remote code execution due to insufficient parameter filtering. User data generated in a particular way is handled by ImageMagick and executes commands in a command-line interface of the operational system. In practice the attack is simple: malefactors may upload a file on a server using standard website functions, e.g., change profile picture.

Joomla RCE
Joomla is one of the most popular free open-source content management systems, which raised the number of vulnerable systems to millions. The vulnerability allows creating an account with administrator privileges, which allows executing arbitrary code on the target system. The vulnerability can be exploited remotely, no special conditions are required. We have additional data on the timeline of vulnerability lifecycle.

PHPMailer
PHPMailer is an e-mail sending library for PHP, it is used in numerous ways in many software frameworks, there are many forks of vulnerable code. The combination of these factors means many potentially vulnerable systems are in danger.

FFmpeg
FFmpeg is a free solution to process media files. A vulnerability in it means a web portal which has it at its core is vulnerable as well. An M3U8 playlist can be masked as an MP3, an AVI or any other type of files accepted for upload by the target system. From here M3U8 handling bug in FFmpeg may be used: it allows to read any file in the system and send its contents to a server controlled by criminals.

Consensus

2016 demonstrated that it is becoming more and more difficult to buy a security solution. **You have to co-operate with your mitigation service provider. You have to integrate deeply.** Even going to a fancy vendor nowadays doesn’t matter as the landscape gets more complex.

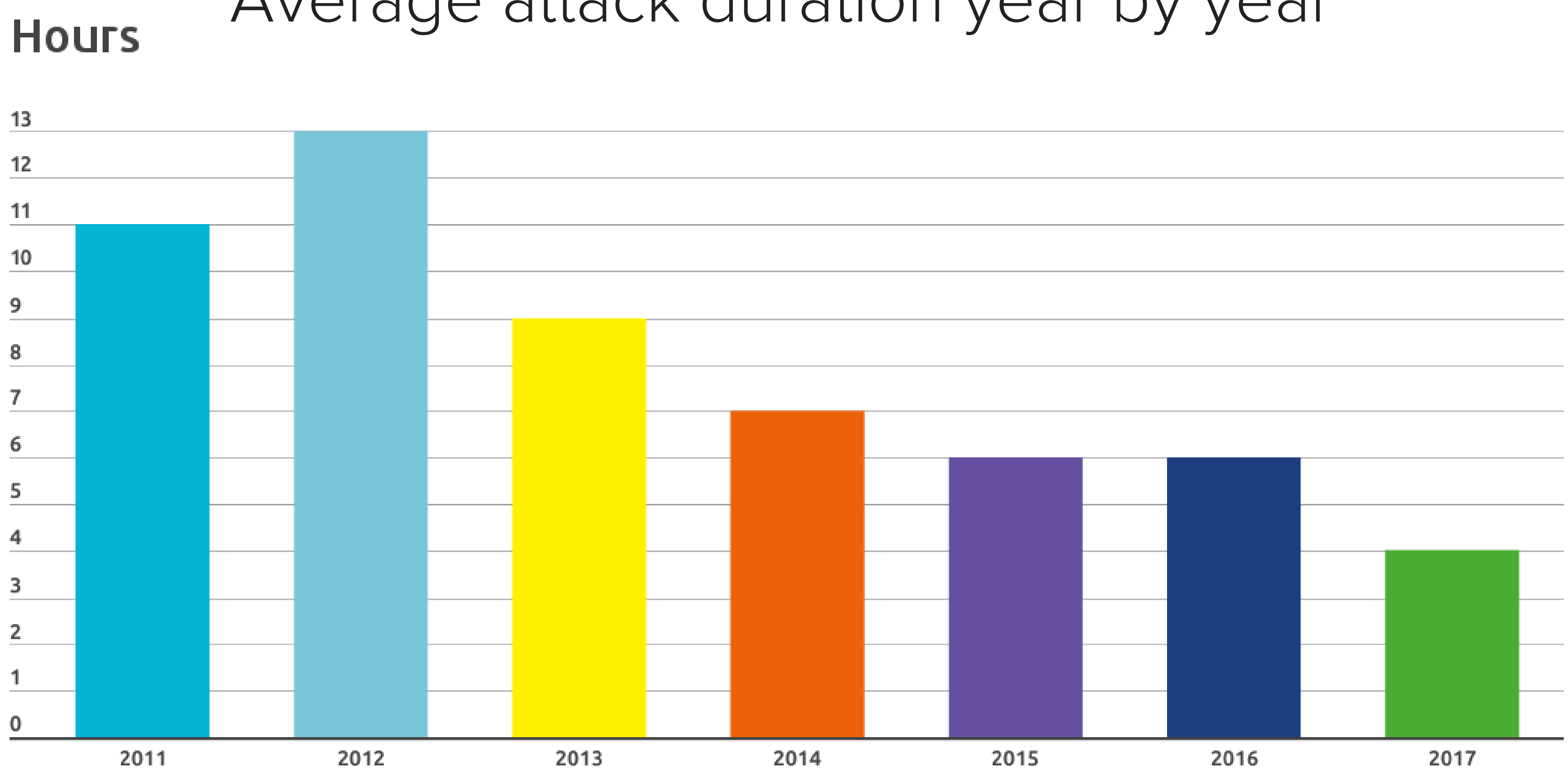
Some companies try to build security solutions on their own, which is expensive and slow. Theoretically, it could also be done by biggest IT-companies. Everyone else just doesn't have the expertise needed.

Only geo-distributed cloud solution providers on the edge of technologies and presence allocation would find answers to all the problems we have on the network right now.

Next: 2017 Forecast

2017 Forecast

Average attack duration year by year



In 2016 it finally happened: an upshift at attack rates and bandwidth ratios occurred

In 2011 we were astonished by a 100 Gbps attacks, in 2013 we were not surprised by 300 Gbps

The end 2016 greeted us with the 1 Tbps attack bandwidth

"Every expert and organization in the cybersecurity industry, including Qrator Labs, have been talking about the same thing for years."

1 Tbps attack appeared to be unreachable for years, but it is already here. What will we have to face in, say, 2019? Nobody could guess, and nobody would get off this battlefield alive, except for geographically distributed cloud services built smart and consciously.

What we see is that bandwidth worth hundreds of gigabits becomes a new norm, and Mirai is only the firstborn of it. In 2017 we expect to see more powerful attacks aiming same vectors at new, unprecedented power since amplification and amplificators step off for the new tribe of raw hazard.

The efficiency of amplification type attacks decreased because the industry learned how to mitigate, and, more importantly, victims started to communicate with other ISPs when troubled and in need for help. Also, this is the reason why botnets like Mirai and Leet, which couldn’t be determined by a single field in a packet, appeared. **On the network level, they both look legitimate.** Handling those malicious networks should be done at a very high speed in a cooperative way for most companies.

There are still some problems in security delegation, along with responsibility to third-parties, but possible losses motivate companies to do that in spite of their fears

"Even we, a DDoS mitigation firm, still, run into people who are not aware and don’t believe in the DDoS problematics."

LDAP has been around for **more than 20 years**, **NTP and DNS for over 30.**

These protocols are all susceptible to being used as DDoS amplifiers, and all were discovered to be vulnerable only within the last decade. New DDoS amplification attack vectors continue to be found in connectionless protocols. A quick Shodan search for open UDP ports results in almost 9 million servers using the SIP protocol, over a million servers using Portmap, and more than 18,000 servers with an open UDP port 8081.

The next vulnerable protocol has probably already been out there for years and is ready to serve as an enabling factor in a DDoS amplification attack.

LG recently announced that every device in production would have a Wi-Fi module enabled, and some devices, like fridges, would get several cameras. Even legacy booking systems are actively exploited as we saw in a report from SRlabs.

Speaking about DDoS mitigation services,
only physically distributed cloud service providers could survive the future

Infrastructure suffers

The main idea behind classical ISPs is to have connectivity, where client traffic is. However, normal traffic values never reflect possible risks: there are criminals, malefactors, and potential attackers in these places, and they go through those tiny uplinks bringing them to a **complete halt easily.**

However, such tiny links could hold critical traffic: for example, a “big national bank” connected to such ISP could suffer because it has those active clients behind this link, who want the service to be available immediately, not “tomorrow” when a potential attack could end (which usually doesn’t).

For small operators everything is much worse — they do not possess wide uplinks at all. Moreover, they could not afford to invest those huge amounts into infrastructure because it doubts their business in general. A 10 Gbps uplink is nothing nowadays. It is only a matter of time when the attack comes and causes damage.

Even 20, 40 or 100 Gbps uplink does not take a company anywhere, bots and DDoS amplification attacks still prevail.

Future is bright only for those who can play defense collectively in the cloud

BGP Anycast clouds have the different design in mind: absence of network between PoPs gives an opportunity for far better scalability. However, the way these clouds were built matters. The ‘classical’ way of a tiny uplink here and huge on there may result in an attack on a small one since it is easier to do damage there, and recently Mirai demonstrated the level of seriousness in finding a resolution.

"Our answer to those problems is infrastructure in such a style, that we do not have those narrow uplinks at all (as a class) and we connect only to the highest tier ISPs in different parts of the world, thus eliminating network traffic congestion at our peerings and beyond."

The attackers’ “infrastructure” is also rapidly changing. In the past botnets consisted of end-user computers only. Now, we observe millions of never-updated routers, smartphones and other devices with default or hard-coded usernames and passwords. In 2016 we saw some financial institutions dropping Android from the list of trusted platforms because of its chronic issues. Two-factor authentication is still recognized as the most secure way to manage finances, but it heavily relies on a smartphone and its screen, both of which are quite vulnerable.

Nowadays there are millions of IoT devices as well, and their security is weak. **As a result, botnets became significantly widely cheaper.**

We expect 2017 to be the year of growing attacks from connected devices: smartphones and TVs

Such a botnet could be cheap to obtain and easy to manage, it would generate enormous profits to its orchestrator at the beginning of its lifecycle. We do not possess any data on the effectiveness of these botnets, but as Mirai demonstrated, the absence of one attacking botnet does not solve the problem itself. Even if Mirai-associated malware and attack vectors could be handled and mitigated in the future, we would still see other botnets exploiting different protocols, weak points, and breaches.

Another popular mechanism of DDoS attacks, amplification attacks, keeps evolving. We have yet to see examples of noteworthy attacks on more new protocols: gaming protocols (e.g., Quake Network Protocol). For example, BitTorrent is, just for now, out of trouble due to hardships of exploiting DHT, though some consider it possible. In fact, DHT has no particular port to defend from in case of possible attack — the same goes for Kad. In the event of a BitTorrent assault nothing would work — not even BGP flowspec or bitmasks.

Newer protocols, designed after 2005
— gaming and streaming —
need a cautious approach

BGP perspective

Speaking about BGP anomalies, Qrator Labs expect them to grow in the direct proportion, as a number of ISPs in the world. Moreover, since IPv6 mass adoption is close enough, we expect a significant grow of anomalies in the v6 network.

Since BGP protocol development does not keep up with the risk growth dynamics, the only possible answer is a proactive monitoring. This does not relate only and solely to the ISPs, but every service, which continuous availability is critical.

"All these changes have one simple conclusion: infrastructure players, including ISPs, web hosting providers and clouds should prepare to the idea that mitigation of a 1 Tbps attack is not something outstanding. This is a new norm we foresee in the nearest future — and its mitigation is a quite costly procedure."

Hacking in 2017

1. Vulnerabilities in enterprises which switch to Agile methods in software development and deploy their code using CI/CD **would be discovered faster.** To achieve proactive defense companies would have to embed security practices in the process of development and deployment.

2. Hacks and network scanning would become massive. The time window between first reports about a vulnerability and its widespread use for hacks would further diminish. More and more malefactors would possess databases with prescanned Internet with data segmented by deployed CMS, frameworks. The most vulnerable IoT devices are security cameras, routers, and NAS.

3. The number of attacks on new technological stacks such as microcontainers, clouds (AWS) **would increase.** The rapid spread of new cloud services and lack of mature practices of their management would create new opportunities for hackers.

What to expect

Most Troubled Industries of 2016 - 2017

1. E-commerce
2. Payments systems and Banks
3. Commercial & Financial Organizations
4. Games and Gaming Platforms

"What would you do when hacked? Having an answer is vital. Finding the right solution is crucial."

The mentality "being hacked is good for your company" is proven to be wrong. Security breaches are widespread and pose the existential threat to businesses. Leaks from Yahoo demonstrated how a company preparing for acquisition could suffer. Two hacks, media outlets reporting about users' data leaked online — and Verizon, the only buyer interested in the deal, lowers the price it is ready to pay for the company. Conditions are against Yahoo, and the company agrees to a less beneficial offer.

Hacks were detrimental for other businesses as well. For Ashley Madison a leaked database resulted in a massive fine from regulators. Shortly after attacks on Dyn and its hours of shameful DNS fiasco, Oracle purchased the company. The last two events are not necessary connected to each other, but it is easy to draw conclusions.

Cybercriminals use what's working best and pursue their goal fearlessly. Two things mattering are time required and the potential cost (both "expense" and "income").

But defense specialists have to categorize attacks in order for correct and effective mitigation, which adds a certain complexity in the work on the right side.

It became easy to get on the wrong path

In the past few years, an ongoing battle of defense and attack tools resulted in more sophisticated and advanced mitigation techniques. What was often forgot is the legacy, the amount of systematic, chronic problems of the Internet, which makes it incredibly easy nowadays to exploit, hack, stress and attack in every other possible way.

An 18—19 years old teen with a grin on his face and a few bitcoins in his wallet could be the most dangerous person in information technology of 2017. This is not related to home or foreign politics of big countries. It would not matter if that teen is from New Jersey or Moscow's suburbs.

> *"In the upcoming year or two we expect to see a nuclear type of attacks on ISPs and other infrastructure. In these situations networks of AS or even whole regions could be damaged and become unavailable."*

Observation tools

Attack and mitigation explanation

Qrator differentiates five attack types, based on the ISO OSI model

- L2 – volumetric attacks;
- L3 – infrastructure and hardware aimed attacks;
- L4 – transport layer aimed (mostly TCP);
- L5-L6 – encryption layer oriented (mostly TLS/SSL);
- L7 – application layer based (HTTP, DNS, XMLGate, VoIP)

Denial-of-service attacks are characterized by a clear attempt of attackers to prevent legitimate users of a service from using it. There are two general forms of DoS attacks: those that crash services and those that flood them.

The most dangerous attacks are distributed. During a DDoS attack, the incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more. That makes it impossible to stop the attack simply by blocking a single IP address; plus, it is tough to distinguish legitimate user traffic from attack traffic when it is spread across so many points of origin. Many attacks involve forging of IP sender addresses (IP address spoofing) so that the location of the attacking machines cannot be identified easily and so that the attack is impossible to defeat using ingress filtering.

Amplificators are used to magnify the bandwidth that is sent to a victim. DNS servers show a typical example of congestion on the target system using DNS response traffic, using a much larger list of DNS servers than seen earlier. The process typically involves an attacker sending a DNS name lookup request to a public DNS server, spoofing the source IP address of the targeted victim. The attacker tries to request as much zone information as possible, thus amplifying the DNS record response that is sent to the targeted victim. Since the size of the request is significantly smaller than the response, the attacker can increase the amount of traffic directed at the target with ease.

BGP is a protocol for exchanging (advertising) routing information between ISPs.

Radar, or monitoring anatomy

"Qrator Labs answers those calls with proactive state monitoring, and this report is aimed at explaining on how we do this."

Regarding volumetric and infrastructure attacks, the main issue is network architecture and network traffic congestion at peerings. **Today, a global anycast network is required to fight DDoS attacks successfully.** Moreover, it is important to design that network and its presence on the Internet with DDoS prevention in mind.

Qrator Radar was created as an internal project aimed at designing a fault-tolerant anycast network with low latency. We tried several third-party solutions at the time, and we found the fault ratio to be incredibly high. **Those could not be used in critical and important applications.** That was the first reason why we started to conduct our research in this area of Autonomous Systems interconnection and network anomalies at interdomain routing level, for ourselves, for company's internal needs.

During the process of investigation, we understood that the industry conceived the idea of such a tool as "impossible," which was rather surprising and that if we succeed, the product could be valuable for lots of technicians and companies in the world. De facto a tool like that is needed by lots of companies, and they use existing ones to get this kind of data. Our idea is that all those tools never worked very well. **That is why we created Radar.**

Nowadays, in 2017, Radar has three main data flows:

— **Autonomous Systems connectivity** (we show business relationships by disassembling paths between AS).

— **Security data on different network incidents** that could happen within AS (amplifications, static loops);

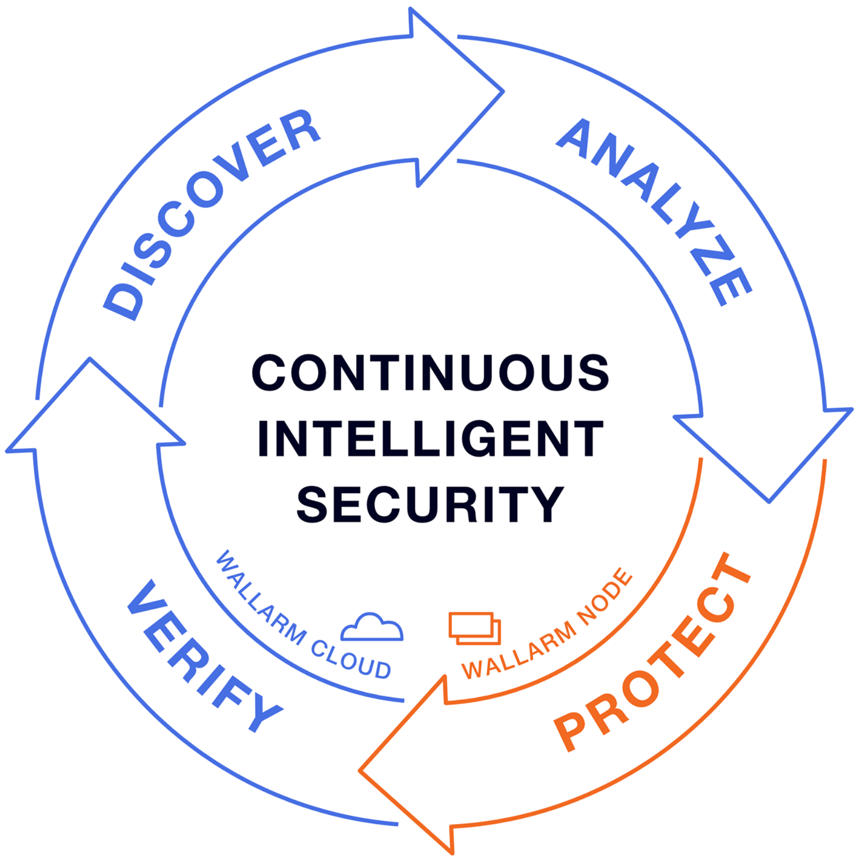
— **Network anomalies** that happen beyond its borders (inter-domain routing: route leaks, MOAS conflicts, BGP Dynamic Loops).

"All this happens outside of AS border, which is uncontrollable and could only be observed separately from the global network infrastructure model but influences the AS directly."

Now Radar could monitor those three flows and update the information once in 24 hours, which we see as a good result. In 2016 we launched a BGP routing visualization tool that works on **a 60- second frequency rate**. This service could also be used as the global looking glass. **During the Q1 of 2017, we are planning to update all other Radar-related services to work at the same speed and refresh ratio.**

Software vulnerabilities, hacks and L7 attacks

Wallarm is an adaptive application security solution which combines Discovery, Analysis, Protection and Verification functions. **Unlike Web Applications Firewalls, Wallarm uses traffic analysis and threat intelligence** to generate vulnerability tests and security rules which reduce false positives and allow security and DevOps teams to focus on vulnerabilities that present real risks.



"Companies tend to ignore the issues of their network perimeter, and that can become a great source of problems at any time. It seems odd, but the bigger company is, the more subdomains it has, the more marketing activities it supports, the less it can tell about what's going on and when at a specific moment in time."

Discover
Discover hosts, domains, and services accessible from the outside, combining deep scanning and data from external sources.

Analyze
Apply machine learning to reconstruct application logic and API schema by traffic. Create dynamic blocking rules based on abnormal data patterns.

Protect
Block unauthorized access, evaluate attacks and alert on high-risk attempts targeted to validated vulnerabilities. Apply virtual patches.

Verify
Analyze and actively replay applications' input/output payloads
to determine if an exploit is possible.

> *"All those parts communicate within one product to make us sure that we see attacks and differentiate attacks from abnormal activity — which we detect very often due to distinctive request signatures, but could tell whether it is a real attack or just something similar. For example, at PHPMyAdmin, you can legitimately write SQL-queries and requests which are not injections."*

About both companies

QRATOR

Established in 2009, Qrator Labs provides DDoS mitigation services and is an acknowledged expert in this industry.

The Qrator Labs expert team has been conducting research in the field of DDoS protection since 2006 and has been continuously improving algorithms, technologies and techniques of DDoS attack mitigation.

In 2010 the company launched its own Qrator traffic filtration network as a technological basis for the commercial service dedicated to the protection of network services from similar threats. Algorithms and technologies used for mitigation of attacks against the web services of its customers are the company's specialty and focus.

Presently, Qrator Labs is one of the leaders in the DDoS protection market. Among its customers are many major companies from various industries: leading banks ("Tinkoff Credit Systems" Bank, UniCredit Bank, MDM Bank, Rocket Bank, OTP Bank, Banca Intesa, National Settlement Depository Bank) and payment systems (Qiwi, Cyberplat, Elecsnet), electronic commerce stores (Lamoda, Ulmart, Eldorado, Wildberries, Citilink), mass media (Rossiya Segodnya International News Agency, ITARTASS, Echo of Moscow radio station, Regnum, TV channels: Zvezda, TNT, Dozhd, NTV plus) and many others.

www.qrator.net press@qrator.net

wallarm

Wallarm develops web resource protection solutions that combine functions of web application firewalls (WAF) and active vulnerability scanners. The products are in demand among the internet companies with highly loaded web applications, operating in markets of ecommerce, online payments, SaaS/PaaS, Big Data, mass media and personal communications.

In 2014 the company was declared the winner of the iSecurity competition held by Skolkovo Foundation among the internet security projects. 2016 Y Combinator alumni.

www.wallarm.com