Executive summary

Of the Qrator and Wallarm State of Network Security Report in 2016

As companies with main focus on DDoS mitigation, and vulnerabilities finding & patching solutions we observed a few changes in the field during the last year.

Incidents related to Denial of Service attacks are again getting media attention. But now a proper attack may threaten availability of the whole regions. The problem again requires increased attention as if we went 5—7 years back in time.

Until the past year it could appear that the issue of DDoS was solved.

But power of attacks and their complexity rose significantly in 2016. In past even powerful 100—300 Gbps attacks caused no real pain. Complex attacks on application layer protocols were rare. In 2016 the world saw 1 Tbps attacks for the first time, while attacks on the L7 layer became much more widespread.

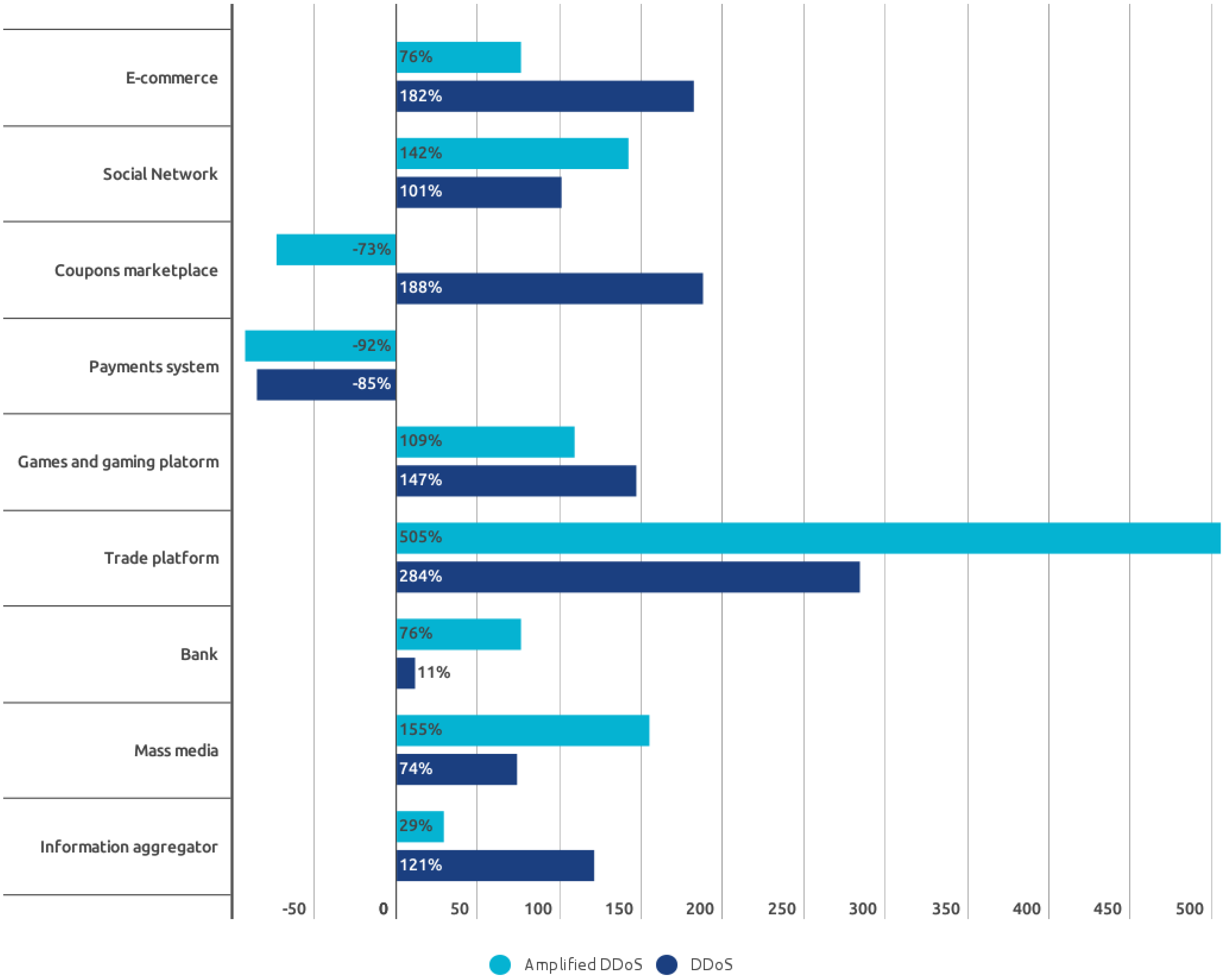
Attacks simplification

Numerous reasons for these changes can be named.

All these years the evolution of IT field went on the path of the least resistance. Companies fought against time and competitors. Cutting corners in the right time and area would result in victory. Security was often left out to create a challenging product.

This represents how the entire modern Internet is formed. The way its protocols and specifications were created gave birth to similar problems.

These problems reached their critical levels of danger. In fact, we are witnessing unprecedented changes of network security as a whole.



State of the industry, dynamics of attacks in 2015—2016

A good example of this is Mirai threat which first appeared last fall. Mirai is a botnet of extraordinary power, it is built on the Internet of things devices — anything from home routers and IP cameras to ridiculous exotics like Wi-Fi enabled kettles. Mirai's threat turned out to be real: blog of a cybersecurity researcher Brian Krebs experienced quite tangible 620 Gbps of a volumetric attack, while OVH, a French web host, sustained 990 Gbps.

We too experienced Mirai last year in a form of 120 Gbps attack.

DNS hosting service Dyn used by many companies from Fortune 500 list suffered the most. Water torture attack on company's DNS servers, TCP and UDP packets on port 53, 1.2 Tbps of traffic from a hundred of thousands of IPs — and some of the biggest websites in the world went offline for a few hours. Protecting DNS is especially hard. Junk traffic usually comes from a dozen of ports (53, 123, and so on). In the case of a DNS server, blocking connections to port 53 means outage in normal operations of the service.

Mirai botnet consisted of devices connected to the Internet with default login-password pairs and vulnerabilities simple enough to exploit. We consider it to be only a first child from a whole generation of IoT botnets. Even solving the Mirai problem these days would not help. At first malefactors bruteforced passwords, now they are searching for breaches and backdoors, sometimes they even reverse-engineer the newest firmware to learn within hours where to hit.

The startup boom and further growth of connected devices' ecosystem is a new field of rich possibilities, where many other huge and dangerous botnets can be created. 1 Tbps attack appeared to be unreachable for years, but it is already here.

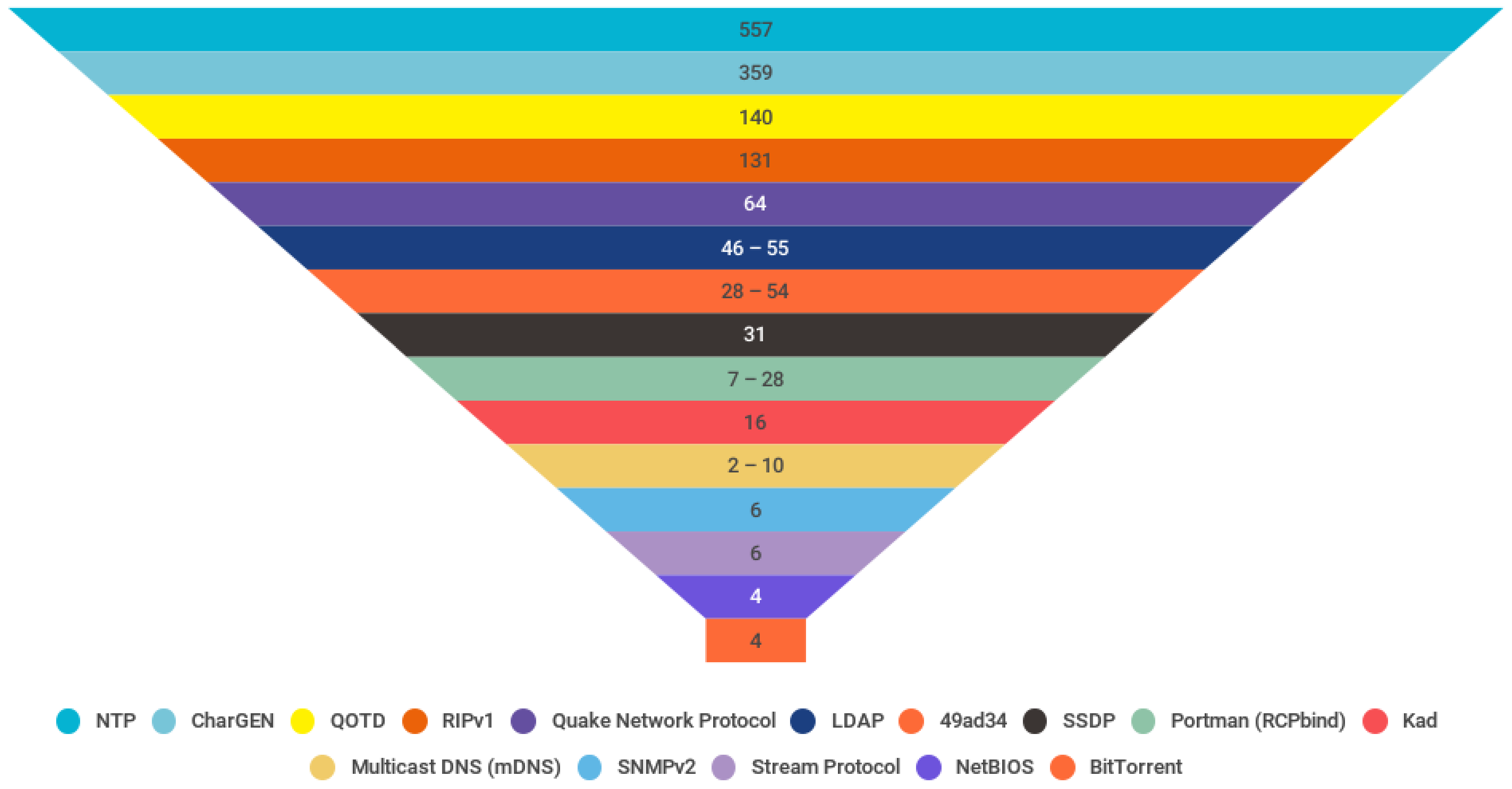
What kind of attacks will we witness in 2019?

At the same time level of expertise and knowledge needed to perform a DDoS attack dropped dramatically. 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. 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.

Amplification and amplificators

To increase attack capacity malefactors amplificate them. By exploiting vulnerabilities in 3rd party services an attacker increases volume of junk traffic being sent and masks IP addresses of the real botnet. A typical example of amplification attack is DNS responses traffic spoofed to be sent to IP of the victim.

Protocol Amplification Factor



Another vector is Wordpress, 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. Pingback vulnerability allows to force a Wordpress server to retrieve an arbitrary Web page anywhere on the Internet by forging a specific XML-query. This attack is called WordPress Pingback DDoS.

Attacks on HTTPS are as simple as on HTTP: the attacker just has to replace “http” with “https.” Mitigation of encrypted attacks requires an Internet connection with a capacity of 20 Gbps or higher and ability to handle L7 wirespeed as well as to decipher all TLS-connections in real time. Those are significant technical demands which could not be met by everyone. This combination of factors is further intensified by huge number of vulnerable Wordpress servers. During one attack hundreds of thousands can be used. Each of them has rather good connection and performance, so its legitimate users will not notice anything unusual.

We witnessed first usage of this vector in 2015 but it’s still being exploited. We expect this type of attacks to rise in frequency and power. Amplification attacks using Wordpress Pingback and DNS aren’t something new, many are familiar with them. In future we may see malefactors exploiting much younger protocols, first of all gaming.

BGP and route leaks

Founding fathers of the Internet had no way to foresee it would grow to its current size. The network they created was the Internet of trust, and the trust was lost during the period of rapid growth. BGP was created when the overall amount of AS was counted in dozens. Right now we have more than 50 000 of them.

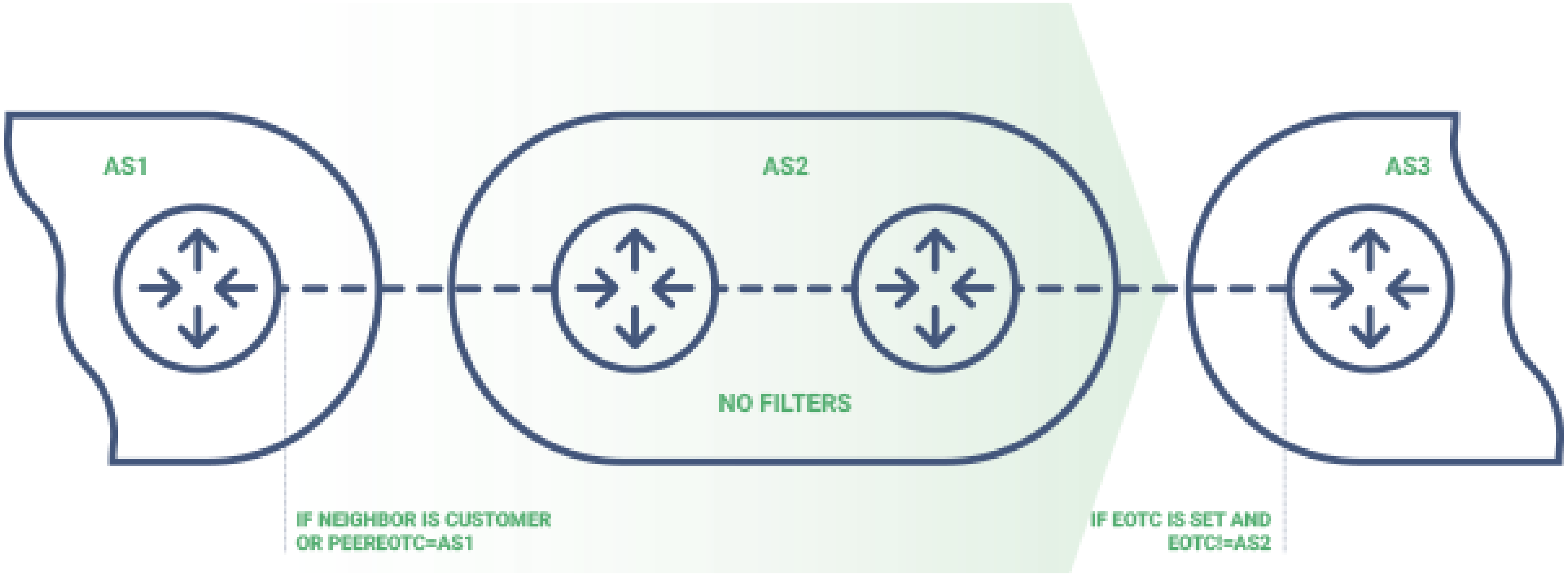
BGP was introduced in late 80's as a napkin draft made by 3 engineers. Unsurprisingly, it answered the questions related to that era. The BGP logics says, “pick the best route available.” There are no money or politics of huge structures in the protocol.

But in the real world money comes first. Money sends traffic from Russia to some locations in Europe, then back to its homeland since sometimes it is cheaper than using a broadband channel inside of the country. Politics do not allow two ISPs who are in conflict to peer directly, it is easier for them to send their traffic using someone else’s services.

Another issue: BGP does not enforce verification of any routing information. That is the point where hijacking issue originates from, as well as route leaks and bogon routes. Not all anomalies are malevolent, often technical specialists do not fully understand BGP. There are no driving license or fines, but we have huge potential for destruction.

A typical example of route leak: 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. At some point this upstream degrades, and you try to shut down BGP session with troubled ISP. You wait for the problem to be resolved. However, the troubled ISP is still announcing your prefixes in all directions and getting a significant part of your traffic. Obviously, this also allows to perform Man in the Middle attacks — this is actually used by some.

To combat leaks in anycast networks we developed a few changes to the protocol and presented them to the Internet Engineering Task Force (IETF). 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' mistakes may influence other ISPs.



IETF develops and promotes voluntary Internet standards. IETF is not a legal entity but a community. This allows IETF to be independent of any legal issues and regulation laws of any country, it cannot be sued, hacked, or attacked. But IETF pays no salaries, everyone participating does it by volunteering to this task force. All activity hardly goes on a priority higher than a "non-profitable" one. So the process of design is slow.

Anyone can propose a new draft — IETF has no membership requirements. The main process takes place at a working group. When the consensus on general subject within a working group is reached, it starts discussions and work on the first versions of the draft. The outcome is reviewed by area directors, their primary goal is to double check everything. The document is then forwarded to IANA since it makes then needed reservation for any protocol changes.

If our draft with a new BGP extension would pass all the hell circles and would be accepted, route leaks would just dry. Of course, malicious leaks would still be here but would be handled in a different way — with proactive monitoring.

Year 2017

We expect to see faster vulnerabilities detection in enterprises. According to statistics obtained using honeypots deployed by Wallarm, in 2016 on average 3 hours pass between first proof-of-concept for vulnerability and further exploitation of it. This time period used to be a week in 2013. Malefactors are getting more prepared and professional. This acceleration will continue. **We expect this period to shrink down to 2 hours in the nearest future. And again only proactive monitoring may prevent this threat and safeguard against terrible consequences.**

Hacks and network scanning are becoming massive. This year more and more malefactors would possess databases with prescanned Internet with data segmented by deployed CMS and frameworks — for example, “all Wordpress servers.” **The number of attacks on new technological stacks such as microcontainers, clouds (AWS, Azure, OpenStack) would increase.**

In the upcoming year or two we expect to see a nuclear type of attacks on ISPs and other infrastructure. In these situation s networks of AS or even whole regions could be damaged and become unavailable. The last few years of attack and defense allowed to develop much more advanced attacks mitigation methods. But industry often forgot about legacy, and technical debt made attacks incredibly easy. **Starting this moment only geo-distributed cloud solutions will be able to survive record-breaking assaults.**

QRATOR

wallarm

Points presented above are only excerpts from our new report on the state of network security. We have described threats listed above and many others much more thoroughly in this document.