Qrator Labs 2017 Annual Report

2017

With information support from Wallarm

Prague, 2018

1

Intro

The steady flow of indiscriminant attacks in the internet wars with weapons of mass destruction has stalled—now comes the time for precision strikes with tactical weapons.

We expect that the current ceasefire represents merely a brief calm before another storm. The Internet is becoming more intelligent with malefactors creating more vectors for potential attacks.

Qrator Labs has noticed increasing diversification of threats from a widening variety of attack methods. The range of critical vulnerabilities on today's web is so broad that attackers can choose from many different methods to create problems for almost any organization. A growing number of tools can operate automatically making centralized command & control unnecessary.

With more and more tools and techniques for launching attacks and various archives getting open-sourced and freely distributed, strong integration with security solutions is becoming crucial for any digital business. Otherwise it is almost impossible to build and maintain a sustainable defense.

DDoS awareness grows with the attack state shifting towards the healthy state of the Internet. DDoS attacks are like sharks in the ocean—you know they are there, even if you do not see any shark fins above the water. This picture describes what's happening in the modern internet, where DDoS attacks occur every minute—they become the new normal, and those serving accessibility are adapting by including such services in their bundles. In 2017 an internet business without DDoS-mitigation and WAF is ceased to exist.

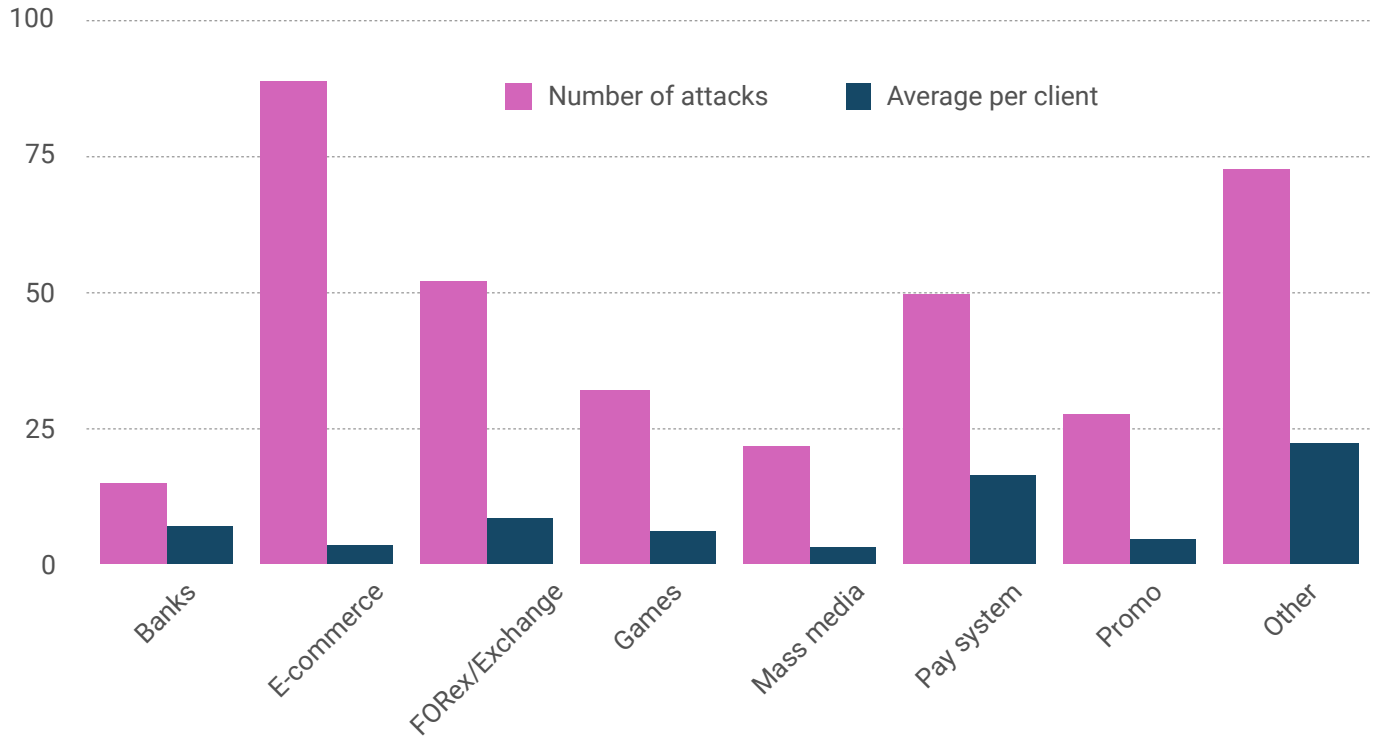
If 2016 could be named the year of botnets and terabit attacks, then 2017 was the year of networks and routing. The incidents, like Google in Japan and Level3 in the United States, Rostelecom in Russia, and many others demonstrate the persistently strong risks from human factors rooted in mismanagement and insufficient automation. A brave engineer who confidently cancels an important automated script could create the possibility of severe issues in internet service availability and accessibility.

In 2017 routing incidents became as infamous as botnets were in 2016. A successful DDoS-attack could render just one, single and separate, web resource or application unavailable, or it could be massive (consider the popular social networks) and dangerous for entire ecosystems using interconnected tools or pieces of infrastructure (hosting, ISP). As we have seen, routing outages could be overwhelming and severe, taking offline almost a whole country. What happens if one day you could not connect to any website at all, making unavailable the electronic communication we now take for granted?

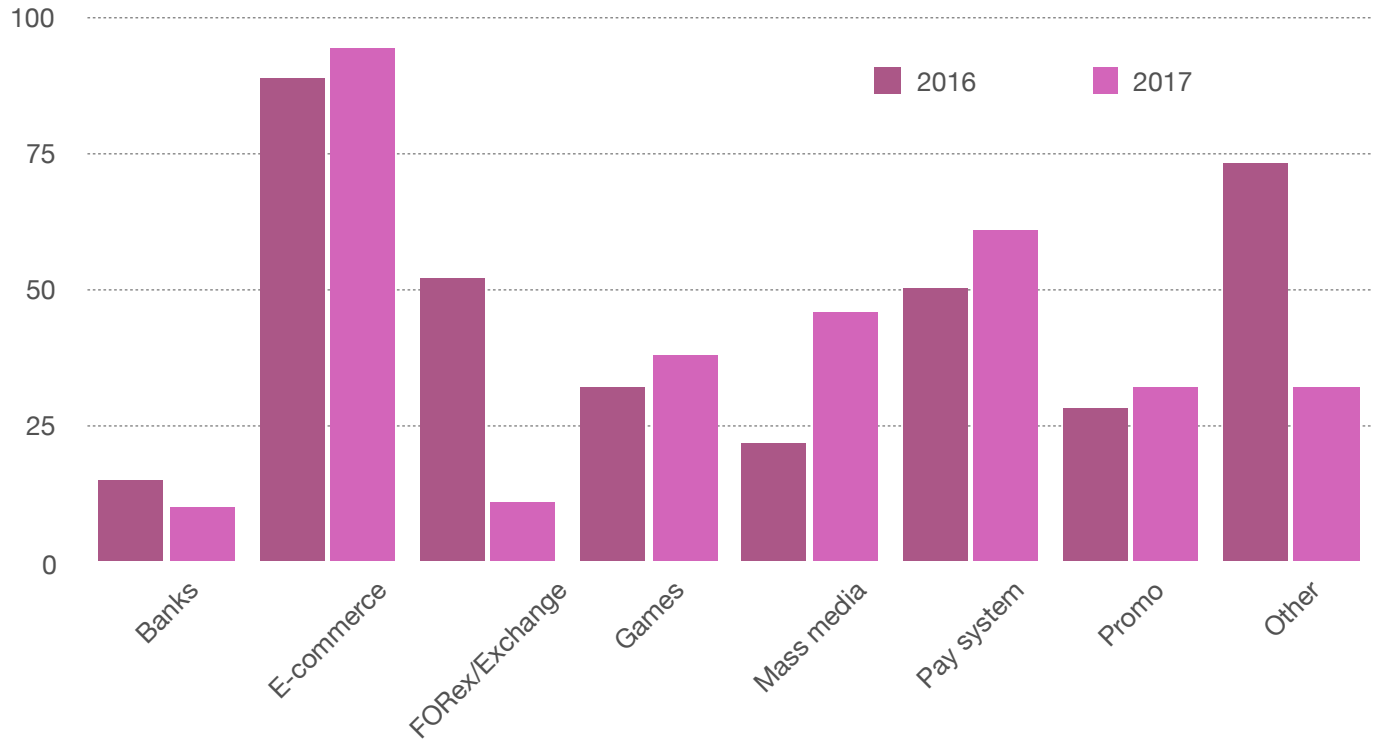
It is now 2018, and you can't just turn off all automation and scripts without suffering consequences.

Hacking as a threat has been overhyped without adequate technical evidence to support the level of attention given. In our opinion, this has only served to mislead the public and complicate the business climate all over the world.

Number of attacks on chosen customer segments



Number of attacks dynamics



2 Internet of Things

Botnets are developed on just a few initial points. If a botnet exploits some vulnerability, it would die as soon as the vulnerability is fixed. If a botnet exists at the level of Trojan, where it is distributed by email in the form of a malicious file, nothing limits its existence since people will probably never stop downloading and opening files from their inboxes.

Many IoT devices are still being hacked by exploiting trivial vulnerabilities, like those involving web UI. Almost all such vulnerabilities are critical, but vendors have limited options, since there is no possibility to deliver a fast patch and upgrade.

IoT hacks have increased since the Mirai toolkit became a standard botnet creation method in 2017. However, an earlier series of botnets had been developed separately and Mirai used some ideas from their code.

The execution of DDoS and other attacks

The main difference between 2016 and the last year is that malefactors shifted their attention from hacking individual devices to attacking the entire cloud via IoT-platforms. The IoT provides attackers with access to thousands of fully capable devices at once, and such breaches could go undetected. This economic efficiency is why we expect such attacks to happen with increased frequency in 2018.

Conflict over vulnerable IP-cameras and other connected devices led to fragmentation of the original Mirai botnet whereby a dozen smaller botnets now control smaller equal portions of compromised devices. Critical issues still exist and the threat remains that all vulnerable devices could again come under one roof.

is a business—a business that does not need New York Times headlines or FBI investigations. IoT botnet attacks have already shown what they are capable of and there is no need to relearn this lesson to avoid publicity. Now is the time for the criminals to quietly try to realize returns on their investments.

A quick dive into how this economy is working could be made with the 2017 rumors from Anomali Director of Security Strategy. Cryptographic ransomware became the main menace in 2017 and forced all sides of the conflict, including governments. (except ordinary users) to pay attention to infosecurity and implement monitoring and early detection tools and policies. As a consequence, we see that among blackhat specialists ransomware has obtained a bad reputation. That is something we saw happen in the DDoS-market earlier.

IoT evolution advanced rapidly throughout 2017. Zyxel modems were recently captured by a version of Mirai by way of default logins and passwords.

The conscience that never awakens
DRWEB

The Internet is a primary communication medium for everyone, both legitimate and "dark," so there is no interest in taking down the whole system.

More botnets, looking at the BlueBorne, could be easily predicted—more in number and scale, more dangerous, more rigid. Looking ahead in the near term, with the possibility of spreading worms via Wi-Fi we anticipate a rise of botnets made for "small" devices, like smartwatches.

We expect to see the disbursal of massive botnets, capable of flooding without exploiting amplification protocols. They can serve as sleeping dragons for someone collecting compromised devices into networks but not attempting any actions. Maybe such botnets are used somehow, but we do not see evidence of activity. Alternatively, there is no possibility for 100% utilization of their capabilities.

Undoubtedly, coordination between engineering and networking communities and government institutions would help prevent huge problems with both IoT and old protocols. We cannot point out any important successes in this area during 2017. It is still everyone's job to mitigate, defend and answer these challenges.

The Attack Vector "BlueBorne" Exposes Almost Every Connected Device
ARMIS

MAXIMUM BOTNET ON 2017

124 000

DEVICES UNDER ONE COMMAND & CONTROL

3

Cryptomania

IoT and cryptocurrencies are so hot right now it is inevitable that there will be some sort of dirty bomb explosion.

Bitcoin in 2017 proved to be a good realization of the hyperledger concept. It is the most hyped product at the moment, but the technology is still searching for a purpose. Every hard fork of a cryptocurrency is a "fail" for the database from an engineering perspective.

A whole new market for ICO hacks has grown throughout 2017. The tendency of attacking during an organization's most stressful moment persists, and with various cryptocurrency startups, these come in the form of hacks or DDoS's, often in combination. If the ICO market grows we expect this trend to increase as well.

Financial excitement levels are high among ICO's, cryptocurrencies and other fintech startups. There's already a lot of money in those markets, but what differentiates this whole new industry from traditional banking is the short-term, high speed movement from plans to execution, with a generation of savvy young people eager to make money. Of course, such ecosystems attract all kinds of crooks and cryptocurrencies suffer hugely from both hacks and DDoS-attacks.

The ICO market is currently more about the news than technology. Before the bad news came to Ethereum, its celebrated founder Mr. Buterin seemed positioned to become a new leader and visionary. But at the beginning of 2018 that still hasn't happened. So we expect the froth to dissolve and then we will see fascinating applications of such technology as the blockchain.

BTC mining pools are experiencing DDoS attacks in the last seconds of each block to spawn additional branches of correct calculation. Cloud wallets are also under fire and we saw several hacks throughout the year. Cryptocurrency mining on foreign machines could be profitable, even for zombie machines like old PCs and servers that were infected.

This blockchain is scaling, but it is still unclear what kind of economy stands behind it, except for supplying the incredible demand for electricity. Serious players have been looking into cryptocurrencies because it is not licensed and there's a lot of hype and young and active people, with fantastic percentage rise and fall. If that is a bubble it could burst, but it is not clear if it is a bubble because traditional laws of economics don't seem to apply directly.

ICOs are of primary interest to both sides of the market. Because of cryptocurrencies and ICO's, a whole new industry of hacking them has emerged before our eyes. There are large amounts of money, and the technical side is rather weak, which we described in 2017. They are being hacked continuously.

In 2018 we will see responses to the events of 2017, especially since bitcoin is now such an expensive commodity that is being widely adopted and accepted.

Attacks on mining pools are also popular; they provide attackers another way to manipulate bitcoin networks and computing power. It will get much worse—nobody knows when or where the rise of cryptocurrency values will end, and the more expensive they become, the more hacking will be attempted.

Some feared that Bitcoin individually, or other cryptocurrencies in general could fail due to some technical mistake in the code. That has not happened until now which is great, but we cannot estimate the probability of such an event in the future.

Browser cryptocurrency mining is something that we should consider because the idea is both exciting and irritating. When an individual's computer power is ultimately taken into the pool, though in case of advertising you could ignore the banner or even like it, which won't happen in the mining scenario. Though some people hate advertising and for them, that is a better option.

Mining any cryptocurrency with Javascript in the browser is slow, even slower than on a modest local PC without added GPUs. However, it does not matter since it provides additional traffic monetization for everyone. Also, hacked websites with some injected code do make some difference. Even some TOR exit nodes swap HTTP adding JS miner for everyone using that particular node. Don't forget that not everyone is blocking scripts in their browser.

Networking attacks on the hyperledger infrastructure (like DDoSing bitcoin mining pools at the end of each block) and cryptocurrencies will grow in numbers. Each complex technology has a foundation, and if there are fractures in it, the building would not last for long.

4

Legacy Infrastructure

The main issues for web services remain the same as they have been since the dawn of the internet: either channels are too narrow, forbidding the normal flow of data or applications are poorly designed, contain too many errors or are written in a generally suboptimal manner.

2017 showed that many different kinds of hardware could be vulnerable to numerous types of cyberattacks. We will see many more incidents involving outdated hardware and software.

Smartphone-enabled attacks could be made by either malware applications in stores or based on vulnerabilities, such as BlueBorne. Browser extensions, network devices (already suffered enough during the last three years) and middleboxes, all could be tested for resistance to attack again and again and would probably fail.

Attackers are well aware of the situation after many years and it is clear to everyone that for any website, either the channel or the application would have some vulnerabilities that may be open to attack. While bandwidth attacks do not represent dire threats these days and could be mitigated in most scenarios even with under-attack service adoption, application attacks could be much more devastating and harder to deal with.

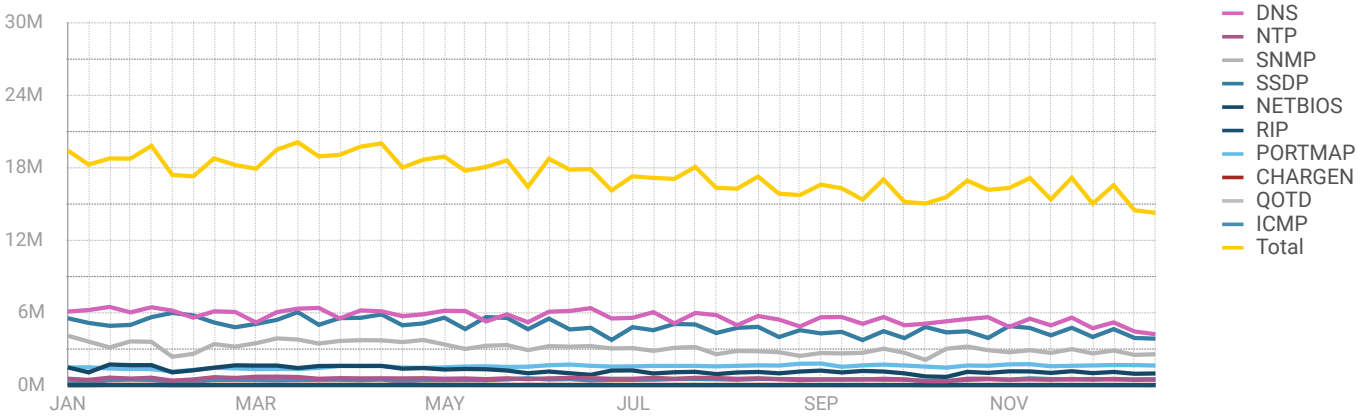
Lately, we have also seen the scenario where everything appears to function normally with the channels and links and the application is well written, however, the protocol this application is relying upon has a severe flaw or even a vulnerability by design. That is a threat of a different order since you cannot make front-end and back-end developers read RFCs these days, this would slow down the entire development process for most companies out there, excluding the biggest ones which make the RFCs.

Usually, people tend not to question the scalability of their applications under heavy load, and we could even say that in 2017 technologies are perceived by a most developers as “highly scalable” thanks to the cloud providing increased computational server power on demand. Depending on who built the application there could be two possible weak points: an attacker could either try to find a specific request that gets them closer to the goal, or they could flood the application with traffic especially for services and applications where high load visitor traffic was targeted and pre-planned requests don’t work. As a result, such targets are attacked mostly with the flood strategy, since it is easier to choke on malicious requests when you already have many customers or other legitimate users trying to access the page or app. In other words, if there is a page that could be requested without any authorization then it should be fully cached.

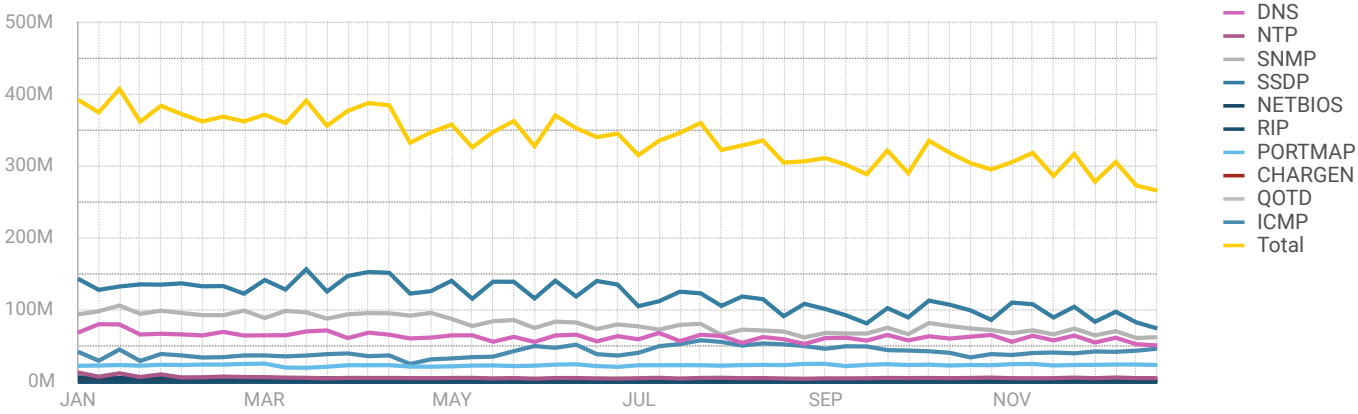
The events of 2017 highlighted these human factors and underscored their importance. Hiring techniques

Human factors always have been, are and will continue to be the most vulnerable points of entry for any company or internet service. On the contrary, the human element is also the strongest point of defense, since people do all the work and everything is in their hands. Known technology issues are closely related since the code was also written by a person.

Amplificators count



Amplificators factor



and internal policies help formulate how people think about their work and company values. The greater the company's revenue, the better it can fund operations and the more it can spend to "buy" solutions to existing problems; but some things can't be bought, and those primarily include employee morale and attention to detail in routine tasks. It can be a strength or a weakness. Architecture could be a massive failure point for any application, and people make it, that is why communication is so crucial for successful mitigation.

Inner Network

Route leaks appear each and every day. We are disappointed by the recurrence of 'fat finger' problems in the networking area. This should not be an issue, but still is. Sometimes it appears as though ISPs don't know what they are doing at all and Brazil is a beautiful country with many more networking problems than any other region of the world.

Continuous tuning of the AS-relation model made it possible to get incident reporting on track during 2017. The networking incident between Google and Japan was perhaps the most severe example of what could happen due to BGP misconfiguration by a big, though single, content provider.

Global route leaks and IP address space hijacks are in the headlines again, but they happen all the time (hijack statistics for mobile networks and content) creating network delays.

Against man-in-the-middle attacks encryption is not the magic potion anymore. Vulnerable infrastructure

It was frighteningly easy to exploit the whole networking world in 2017. All attention was drawn to routing incidents and the ability to successfully intercept any traffic for future or even current needs makes BGP misuse highly probable.

In the case of the BGP, we need to be extremely careful, because the possible damage could be immense. Since BGP manages all traffic from one AS to another, we are talking not only about increased latencies for users but more importantly – the possibility of Man in The Middle attacks on encrypted traffic. Such incidents could affect millions of users, entire nations even.

provokes new kinds of attacks with certificates, cheater proxy, Windows DNS vulnerability and finally things like Outlook sending plain text messages along with encrypted duplicates.

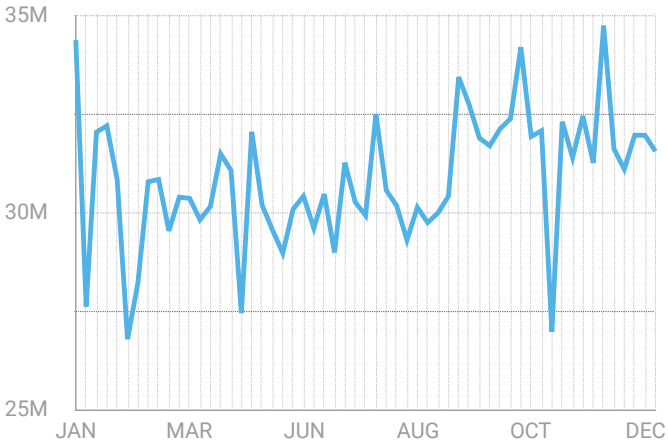
BGP, DNS and local managers of those protocols are still among the most significant network vulnerabilities. There remains false hope that everything built upon them would be safe. But lots of threats pervade the web: amplificators, though declining, still exist, enabling an attack to quickly reach 1 Tbps bandwidth, since there are lots of unsecured networks. However, since amplificators are well known as a problem and relatively easily detected, they are becoming less and less prevalent. Old hardware is either patched or decommissioned by now.

Network operators with their own autonomous systems, must become fully aware of what is happening within their perimeter. Vulnerabilities still could appear and must be patched, There are ways to deal with network incidents too if they are fully understood.

More specific prefixes are always preferred during routing. And during BGP configuration the slightest mistake in the IP address can lead to bad things happening. Still, members of the BGP community manage to build trusting working relationships. However, the adoption rate of new technologies, like DNSSEC (15% in 2017) or RPKI (7%) is slow, and we think that is because AS operators feel satisfied with their current solutions. There is not enough motivation to perform updates because of incompatibility risks and increased expenses. Adequately securing users requires capital investment that does not lead to tangible revenue growth.

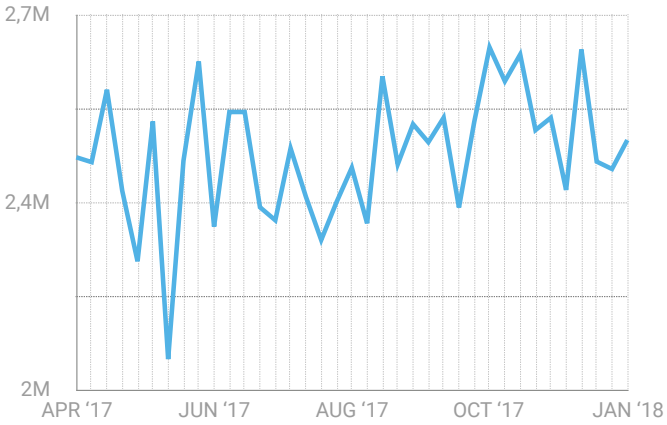
Of course, new tools are supposed to help those AS operators, but we do not see that happening. In addition to the endangered protocol, we have software

Static Loops in 2017



It doesn't get any better—there are 30 millions of active static loops on average. 0,7% of IPv4 address space is affected by static loops on a daily basis.

BGP open ports



BGP open port became the vulnerability only recently, with Qrator Labs.Radar team counting such open port as the potentially exploited possibility for a hacker, leading at least to the autonomous system incorrect work.

with serious security issues. With open source products, we realize there is controversy. A popular open source routing daemon has many more features, as well as vulnerabilities, than the old legacy one that was developed by a small group of people.

Network development is characterized by slow processes within organizations like ICANN, IETF, and IEEE and a lack of will from strong corporate players like Amazon, Microsoft, Google and others to work together with ISP's of all sizes on necessary

Content is the new king—those internet-companies that mainly deliver content that originates from users within a network on their platform, like Google, Amazon, Facebook and thousands of others are now starting to build their networks. A prime example is Microsoft this year obtaining a first trans-Atlantic fiber cable for Azure. That is because even before cancellation of Net Neutrality, networks were not free—it has always been necessary to pay for global delivery of content. The networking community will recall the peering wars, which bear strong resemblance to traffic shaping and elite access speed to prime content providers. There is a clear trend of content providers wishing to own their networks—Tier1 ISPs are already often getting bypassed.

improvements. Instead, we see the Net Neutrality Act compromised along with the increasing isolation of each of these network players.

We still live in a world of the open network, but this is increasingly to be appreciated as a luxury and not taken for granted. In 2017, the fact that anyone could get an LIR status and own an AS, thereby becoming an operator is excellent and deserves to be highlighted.

In 2017 we still saw IPv6 providers without global connectivity, because nobody cares. From a technical point of view, an autonomous system is not obliged to peer and exchange traffic with each other. This toxic pattern could leak to the IPv4 world now, with all everything going on around Net Neutrality.

Who Controls Traffic?

MitM is an example of traffic being intercepted between the client and the server. The practice is well known since the earliest days of networking when correspondence was intercepted to access secrets during wars, negotiations or commercial competition. Much

Man-in-the-middle attack
WIKIPEDIA

What actually is the HTTPS protocol? The "S" stands for "security" provided with authentication and encryption. The authentication means that the certification authority verified the owners of a given website.

has changed during this time… except for this. Nowadays traffic interception occurs in the pursuit of such aims as data or credential theft and surveillance.

The common perception of traffic interception is of a distant physical operation, like splitting fiber optic cables somewhere underground far away. Although this could happen, it isn't the most frequent practice. Since the revelations disclosed by Edward Snowden, popular interest in privacy and security questions has grown significantly, and not just in terms of illegal government surveillance. The arrival of Let's Encrypt with its free SSL certificates is but one example of the market response to this particular trend. Without such public interest, we would not see 62,1% internet adoption of HTTPS, according to the SSL Labs statistics.

In 2017 we saw several vulnerabilities enabling MitM attacks of various types, including:

— WPA2 key reinstallation attacks
— Windows DNS client allowing the forgery of queries and compromised code execution
— Outlook 2016 sending plain text messages along with the encrypted ones

HTTPS is vulnerable to the man-in-the-middle attacks. Lots of people tend to think, that HTTPS, because of the authentication and encryption, is invulnerable to all attacks if the certification authority works correctly,—including interception by someone in the middle of an HTTPS-session.

But what often gets forgotten is that MitM attacks on the certification authority could involve the crooks communicating with the certification authority instead of rightful owner, thereby supporting a simple HTTP session with the victim instead. The attacker makes

Route leak is the most common result when attackers discover a mistake caused by human error and it can dramatically impact web resource availability by cutting access for large numbers of users, possibly millions or more. Since almost any route could be advertised by any AS we've seen many such incidents during 2017, There are over 60 000 active AS'. "More specific" paths lead routers to prefer potentially malicious routes where in the end all the data could be, at best, dumped.

the certification authority think that he is the website you are trying to access so that it signs the certificate enabling the attacker to continue with the victim.

How is traffic intercepted on bigger scale?

DNS and BGP are the two main traffic control protocols. It should never be forgotten that the internet is established on the basis of trust, and this fundamental vulnerability is now often being corrupted.

DNS spoofing (DNS cache poisoning) is a technique that involves misdirecting users to a compromised website instead of the real one by forging the IP-address behind the domain name.

BGP which is a standard interdomain routing protocol is in trouble. As a protocol based on trust it could be misled by an AS with two possible consequences: hijack and route leak.

We hope that the BGPSec that finally obtained RFC status in 2017 will be adopted much faster than the DNSSec, which has seen only 15% adoption since 2005.

Currently, every 20th prefix is experiences outing incidents on a daily basis. The Google-Verizon incident in Japan was the most notable example of such an attack in 2017. It resulted from a simple misconfiguration and led to terrible consequences in form of inaccessible websites for Japanese users.

Latency increase is the "best" possible consequence of a hijack and route leak with total AS failure being the "worst".

3 massive routing incidents happened in 2017 and disclosed by the Qrator Labs.Radar team:

1. What happens when a bank plays the IP-transit game? Unavailability for all parties involved.
2. Internet Service Providers are born each day, but once in a while the one born to hijack appears in the wild.
3. At the end of August 2017, a colossal routing incident broke out. Its consequences had such impact that Internal Affairs and Communications Ministry of Japan started an investigation into what caused such a large internet disruption.

What happened the day before was Google leaking prefixes from its peering partners to Verizon, where it was propagated to a butch

Attack (except bruteforce) types

SQL Injections	21%
Remote Code Execution	36%
XSS	38%
Path Traversal	2%
Others	3%

Bruteforce attacks

Bruteforce and credential stuffing	97%
Credential stuffing	2,5%

Attacks distribution by type

These attacks are separated into two big categories: application vulnerabilities attacks and bruteforce attacks to make it more clear, where the vast majority of dangerous requests is.

When Bank Plays in IP-transit Games
QRATOR LABS. RADAR

Born to Hijack
QRATOR LABS. RADAR

of other operators of various size.

Since Google leaked a lot of more specific announces, that are not visible in global BGP routing table, some networks may have experienced a significant increase in traffic delays or even packet loss. For example, the severe impact had experienced AS4713 (NTT OCN), the most significant service provider in Japan.

That particular example showed how severe and scalable could be the routing leak/hijack consequences.

When software becomes critical infrastructure. DNS scaling

Even before the WWW era, Domain Name System was represented by the host file, containing translation of the domain name user access with the server address. At the end of 2017 DNS performs different forms of load balancing (round-robin, geolocation based and other), in addition to being the backbone of the global Internet with root name servers operated by ICANN.

How could a DNS subsystem actually be handled? There are two general options:

1. It could be bought as a cloud service
2. It could be built with internal resources. There are several reasons for not engaging in the internal development of a DNS-management device.

First of all, there is no standard scalable solution that is adopted by the industry for managing the DNS subsystem.

Domain name system management has grown into a separate market niche where considerable resources have been deployed towards the development of proprietary tools and solutions.

Another issue with the DNS is that geo-databases containing data that's expected to help users build reliable DNS management subsystems actually does the opposite. Information given in databases like MaxMind is actually not 100% correct. In 2017 we conducted separate research based on the RIPE Atlas set of tools and found that the rate of mistakes reached 4,6% for Maxmind and this was the best result. 5% of users were directed "somewhere else" by the DNS based on their geolocation parameter.

In 2018, DNS is a highly dynamic system, and this dynamism represents an issue itself. An API based configuration management system is a vital necessity, allowing fast provisioning, policy management and statistics overview for the whole system.

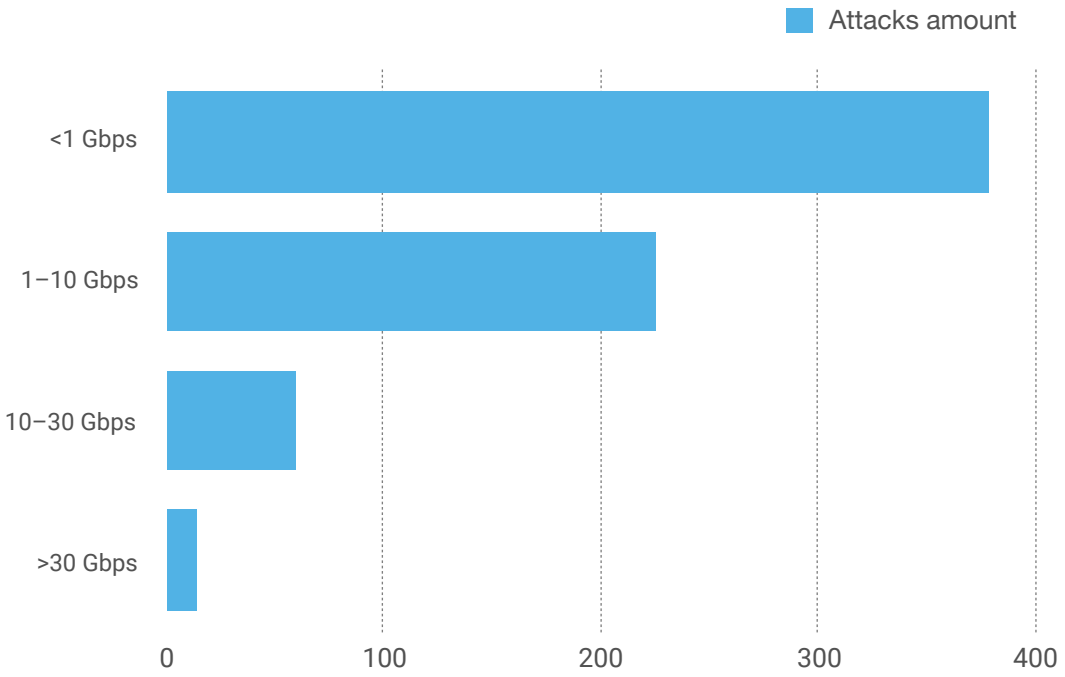
The issue of handling possible failover with the TTLs we have in the DNS is an interesting question, since the lower we set the TTL, the higher we load the entire system and as mentioned, it's not intended to process heavy loads of requests. Last but not least, a complete infrastructure package is crucial to maintain a stable internet business of any sort.

There are several major DNS cloud providers and as one of them, we at Qrator Labs recommend anyone seeking more control over the domain name subsystem in a given digital business to diversify. With the help of SRTT (Smooth Round Trip Time) it is easy to handle two or three separate providers, which naturally provides backup, besides improving latency in

In 2017 Qrator Labs internally tested different open-source servers handling DNS and the results were not impressive. Since DNS queries and responses are not heavy, we expect that the servers are not heavily loaded most of the time. Because of this DNS servers were never meant to be high-powered. And this is an important vulnerability these days, as the 2016 Mirai water-torture DDoS-attacks on the Dyn DNS provider proved. Though the latency of the DNS answer from a given server influences the speed at which the page loads for the end user, it's inefficiency is the truth we've been living for decades now.

In 2017 we realized that the critical responsibility is hiding in the product API. Nowadays all clients want a working and fully functional API, and this need cannot be underestimated. An API is a vital part of our filtering network, but different types of developers and engineers see API's and such requirements differently. Dropping the API is almost equivalent to blackholing the whole network. Because integrating customers into filtrating services requires a great deal of effort and it is a real-time synchronized system, making it difficult to tune in case of emergency.

Amount of attacks vs. Attacks bandwidth



getting a response by the end-user.

Application layer

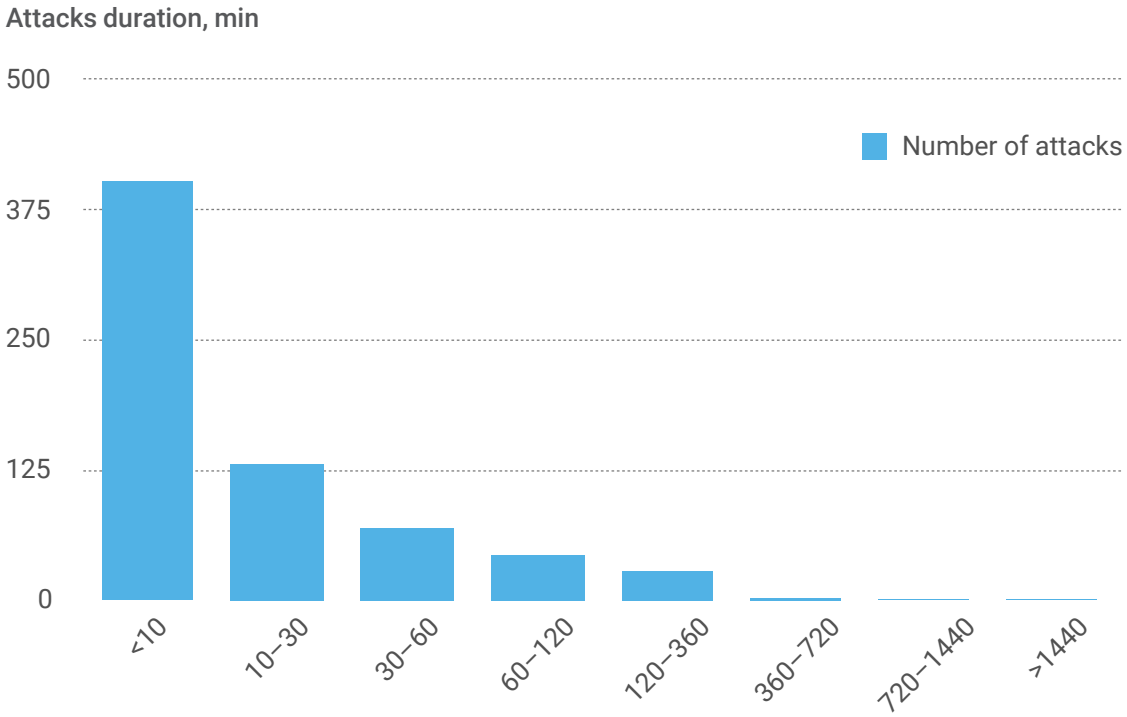
APIs become more and more critical for the more significant customers—they are more professional, and want to have more control over traffic scrubbing and filtration.

Probably most notable are not the attacks themselves but the progress we as vendors of the security solutions have made in learning as we begin to cooperate and communicate, not just compete, in order to mitigate dangerous threats, like botnets. When they start to appear, threatening the existence of entire industries not just "naturally selected" companies, cooperation begins on multiple levels: formal, informal, B2G and B2C. We have already seen success in suppressing the botnets deployed in 2017.

As the DDoS landscape evolves, Qrator Labs is adapting to the changing techniques and methodologies. Nowadays, we need to tightly integrate with our customers to build secure solutions since bypasses are a real problem. If any payload is not analyzed, there is a stress point attackers will eventually try to exploit. Defensive measures were always complicated, but we are troubled by the speed at which malware exploits vulnerabilities and other malicious code spreads. The more prominent a security company is—the more time it takes to provide software and equipment with proper upgrades. Attackers and other malefactors do not need patches since they could have an internal picture of how your solution works and evolves.

L7 attacks are as dangerous as they were before. If you are an enterprise with a dedicated L2 channel to your connection service provider, it is only a matter of time before any single piece of unsecured equipment or third-party service provider connection is exploited. Commercially offered DDoSs were quite complicated in 2017—something could be bypassed, something hacked, eventually, the damage is done. 2017 again showed that Windows-based botnets never disappeared. The effects of WannaCry, Petya and NotPetya could be re-created as a DDoS attack, when a subtle software manages the traffic generated from a single computer within a strong network. In our view botnets are becoming bigger—We may be nearing a break-out point where new versions of malware networks assault the internet.

High-bandwidth attacks with Windows-based botnets made last-year's joke about 1 Tbps L7 attack a sad reality we are seeing more often. So hundreds of application layer Gbps could become a reality in 2018. Right now everything that could be broken with such of attacks (application layer) dies before the offending



Censorship or as we call it "the blockading" of foreign internet resources will be seen in more countries all over the world. Human history shows that integration and cooperation are generally the beneficial as elements for developing international relations. A complex solution benefits from diversity of participants in its creation.

bandwidth reaches such levels.
IoT devices are becoming concentrated on IoT-Platforms, a process that we expect to be accelerated next year to enable simple device management, orchestration, and other steps intended to make life easier. We fear the inevitability when such devices and subsequently their platforms are hacked and millions of devices are compromised.

There is a strong chance that end-to-end encryption is going to be adopted by almost 100% of internet players, projects, resources, and services. It is both positive and negative since governments are highly interested in preserving communication open to them, struggling the efficient encryption all over the world.

The next big thing that troubles us is a political conflict over the "worldwide network control," which we regard as highly possible. Lots of countries want their own, clean and free, internet. What they do not expect is to bear all the expenses, including those related to developing new protocols and providing compatibility. This is very difficult and it is unclear why someone is breaking something that works in an attempt to build something that will not work.

Big Data and machine learning in the form of neural networks have arrived, and we benefit from many new techniques with their help. There remains much to be done, since the current neuro-network and big data applications are mostly in entertainment and advertising. We need to build a more reliable network and try to apply the new capabilities to solve greater problems managing tasks with lots of variables and flows in real-time, like traffic control.

Quantum computing is also developing quickly such that talk about "the end of cryptography" is often heard. However, for now, it's only talk and conjecture.

Network upgrade

BGPSec is becoming the standard, and this is good news for the whole industry. Call your vendors, ISPs, relatives and tell them they should take a look at the specifications of this protocol.

As leading contributors to the IETF draft for BGP open roles, Qrator Labs plans to integrate with the BGPSec to provide full protection against metrics manipulation and route leaks. We have been waiting

for the BGPSec for five years, and it still needs some modifications. Nevertheless, it is vital for all BGP users.

BGP and DNS will be viable and fundamental to internet architecture in the near future. DNSSEC is also getting closer to adaptation because there are many problems with the stability and security in the current version of the domain name system as we were already seeing in 2016. DNS is not 100% reliable—DNS answers could be forged, resolvers could be in the hands of different people, governments, so a DNS-based internet in the future could not be viewed as a space for free-speech and free-flow space. States take advantage of the access point; ISPs are also known to manipulate DNS responses in order to generate additional cash flows. In 2016, we saw that the DNS is vulnerable, and in 2017 we saw vulnerabilities exploited on a mass scale, though not always "criminal" by previous definitions of the term.

Not only HTTPS, but the DNS could also be encrypted.

- **A Encryption (DNS over TLS)**
- **B DNSSEC**
- **C In 2018 we expect local implementations of upgraded DNS protocols**

It will likely take another 5 years to clear the graveyard DNS spawned during its lifecycle.

Technological modernization is the only way of upgrading the situation to maintain the general well-being.

We are pleased to see Atlas RIPE getting more use. IXes has started monitoring outages since they are now interested in "what's going on outside of our network" and news networking incidents drove this change.

We do not see many new players in BGP monitoring. Radar performed considerable analysis of the data from the biggest network multihop BGP sessions—more than 400 feeds worldwide.

There is no alternative to monitoring what is going on with your address space and anything that can influence it. The faster we react to an incident—the less it spreads, which means less traffic will be redirected to the broken or possibly malicious source. Of course, integration of monitoring systems with some management consoles and automatization of management are the current trend we see. With the commoditization of hosting and ISP services, more and more people have never learned how networking protocols can gain access to their controls.

The networking market comprises three large groups: hardware and software vendors and their customers. Such vendors as Mellanox are doing a great job of supporting Switchdev. Vendor-specific locks were a sin of the networking industry, and with the improvement being made to Switchdev users will be able to cooperate on that particular operating system level as well. With 100Gb interfaces, the speed, and amount of data would increase dramatically—the opposite of latency.

Models and internet modeling, precisely, is a very hot topic. We saw some acquisitions recently (BGPmon, Dyn) pointing to the internal use of such specific tools. Those who operate large BGP anycast networks probably have (and if they do not, they should) their own models and network analysis and architectural tools. Google, Microsoft, Amazon also should have models available, since at their scale it is hard to adequately predict network behavior in real-time or close to it.

Other protocols

Individuals and companies mostly develop new tools and protocols for their own use. There are many working groups in IETF, but they hardly communicate with each other. So the effort to develop and create a new internet is fragmented. New transport—QUIC, mostly solves the problems of Google. Facebook open sourced its routing platform and makes proprietary hardware, like DWDM and router boards. Some companies reward their engineers for each paper submitted to engineering organizations. IETF is an organization that ISPs, vendors and other internet companies approach to solve problems that benefit the whole community, so it is worth monitoring closely. We have already seen what happens when the protocol is designed to include a flow, originating in its RFC—that could not happen ever again. IETF changes in

Google's network is also an SDN using BGP for intercommunication. More companies are building unique combinations of services using well-known old protocols. Looking three years into the future, we anticipate two black boxes communicating through hopefully some IP-transport system, but we do not know what will be inside the boxes. There have been other developments: LPWAN is an exciting example of a technology that doesn't rely on v4 addressing. Let's not forget that MPLS is transport-agnostic. OpenFlow is increasing its presence on the market. HTTP/2, except for all the controversy, is being adopted quickly, or at least that is what is being reported. We wish that this trend of ecosystems closing in upon themselves would stop. What we could definitely say is that BGPSec release is good for everyone.

time, swapping vendor as core participants for active engineers from different kind of companies, involving more people with different views into common aim.

The old protocols we rely upon are exceptionally scalable, but not at all secure. That is what we call the legacy, which will probably stay with us for another 10 years. People always want quick gratification, so there is a chance of adoption of certain things that benefit the industry even when partially adopted. It is unrealistic to expect that 100% of the network would implement an upgrade to one single solution.

Unfulfilled promise could result in lots of problems, since sophisticated technologies are often developed behind or on the top of other complicated systems without fully understanding how everything would work as a whole.

IEFT BGP draft

We hope that in 2018 our draft will reach RFC status. The Radar team is investing substantial effort to make the BGP extension suitable for of the entire ISP industry.

5

Legacy Infrastructure and Intranet

2017 was a year of many hacks. From encrypting malware pestilence to exploiting the archives of Vault7 and ShadowBrokers, in addition to notable "human factor" data leakages, with Uber and Equifax being two examples.

It feels like a street gang got control of the arsenal of the most advanced military division in the world. We believe the ransomware cryptoworms were a distraction, and the amount of bitcoins transferred is the proof. Most probably we saw first shoots of an exploitive class, but it will take some time to know for certain.

The Internet is becoming even more of a distribution channel for contagion. It is like being in a crowd where everyone has some dangerous infectious disease, anybody joining the party is vulnerable.

There have been many attacks lately, and they are becoming increasingly dangerous. As we said, in the right combination, with millions of pre-scanned IP-addresses and domain names when a new exploit is released a wave of hacks follows. In open-source, this happens all the time especially as security and all other update logs are public and followed. After important patches are published, it takes just a few days for criminals to prepare new exploits and start attacks. It does not necessarily mean that huge numbers of applications would be attacked—there are 3 billion Wordpress sites, and only 100 000 of them might be affected. But this is still a significant number and significant damage would be seen. IPv6 contributes to spreading attacks with endless proxy and tremendous computing power. Everything happens so fast that most equipment defenses and updates cannot stay ahead of the bad actors.

There are many mistakes made in setting up access for backups and databases resulting in data leaks.

Brute force attacks are also increasing since there are still lots of people with simple passwords and their numbers are not decreasing with time.

Encryption malware epidemics are the current trend, but the same enabling vulnerabilities could be used for DDoS-attacks, which would be an application layer assault over the internet.

Nobody updates, even though the terrifying stories appear daily. Ransomware, encrypting all data within business networks, home computers, hospitals or government agencies, can interrupt work for thousands.

Of course, antivirus programs can be installed, but strangely, they do not prevent such epidemics. Bigger savvier companies try to control everything inside their network perimeter, but it turns out they do not have the power to fully achieve the goal.

Shadow Brokers' exploits worked like a vaccine for old devices connected to the internet. We should take care of old PCs since there are lots of them sometimes in surprising places where people depend on them, What's more important is that they are critically vulnerable. Vault7 did the same, and hopefully, in the future, such efforts will continue.

Vulnerabilities in applications always were and are caused by mistakes in planning the architecture and logic, orchestration, and administration.

Despite strong intentions regarding security, investments in training and advanced products as well as other measures aimed at improving general information security, the actual security level at any given company comes down to the human factor and the degree to which the lessons are learned. The human factor is consistently the primary reason incidents occur.

The companies developing modern browsers invest great efforts to inform the public about unsecured websites, popups, and downloads, which have always been ground zero for epidemics. A significant amount of traffic on the web is encrypted with HTTPS, and people now pay attention to the absence of a certificate, thanks to browser alerts.

Vulnerabilities

Everything is vulnerable. So the real talk should be not about "what's most vulnerable" but "where the vulnerability can be found earlier." Where there are vulnerabilities—there are attacks. Moreover, we have common technologies that can replicate weaknesses, patching one and opening another—and attackers watch this activity closely. They know that the more significant a vendor is, the more time it will take for them to develop and deliver a patch.

The Cloud is already a legacy system with issues that are being inherited by new generations of technology. The Uber and OneLogin leaks started with the Amazon keys being publicly exposed on Github or elsewhere.

Another serious issue is the situation with MongoDB, Cassandra, Memcache and other databases in use. When administrators forget to set an appropriate level of security attackers will find those holes. This was the case with the Ai.Type smartphone keyboard when it lost the data of 31M user accounts with almost key logged activity.

Attack vulnerability types

XSS	50,24%
Information Disclosure	40,82%
SQL Injection	2,78%
CSRF	2,12%
Remote Code Execution	1,62%
Open Redirect	1,23%
Path Traversal	0,66%
XXE (XML eXternal Entity)	0,41%
CRLF Injection	0,12%

Vulnerabilities rating

Found vulnerabilities distribution doesn't change much year by year. Cross-site XSS is traditionally the most used vulnerability. Credential and information disclosure (misconfigured GIT repos, no authorization databases) is the second worst. Injections and first of all SQL-injections are on the third place.

Old software

In 2017 78% of WAF users found vulnerabilities tied to outdated software. Average time of patching them is 15 days.

31 Million Client Registration Files Leaked by Personalized Keyboard Developer
MACKEEPER

Legacy equipment is highly vulnerable and it is entirely unclear for now what to do about it. Old hardware is trouble because it cannot support newer protocols, and at the same time, there are situations when particular equipment cannot be upgraded. That is a mess.

93 DAYS

AVERAGE TIME BEFORE CUSTOMER PATCHES VULNERABILITY

The Uber container key leak was probably the most serious incident of all. Petya and WannaCry were extremely serious epidemics that showed that the borders of the internet are porous and malware that spawns in one country can quickly find its way to others.

It is also noteworthy that some vulnerable functions and applications are being shut off by default in browsers, Flash being the most widely known example. For developers too—we have seen many changes to PHP and MySQL. This helps, as developers do not have enough time to manage their settings properly every time. If more software developers supported this useful practice, then many web applications would become more secure.

Struts exploits continue to happen, and in 2017 we saw the fourth one. Since Struts is a common platform, it gains much-unwanted attention and the Equifax breach is a notable example as the company was building its application with this framework.

Platforms, such as the Struts framework mentioned above, or Rails, are also in the scope of research by several interested parties. Since many applications are built on them, it is more productive to focus on the extensive range of opportunities. When a random code sent with a request is executed, there is no telling to what extent this could be exploited—whole industries and markets could be taken down for hours or even days. To protect our customers from both known and yet-to-be-discovered application framework vulnerabilities, we incorporate technology from our partners, Wallarm, to provide real time anomaly detection and enable virtual patches for known issues.

Lessons Learned from the Equifax Disaster
WALLARM

6

Security systems bypass

Bypassing security systems is becoming the new trend in cyberattacks. The question becomes how to mitigate this scenario, when an expensive system suddenly becomes ineffective, including such products as WAFs, DDoS mitigation services, IDSs and DPIs. Almost any complicated technology could be bypassed these days. Integration is the only mitigation—it is a protective layer of armor.

Not selling lousy integration could be a good thing for your company, since an unfiltered attack does not hurt only a single client or a customer; it first of all questions the service itself.

Public tools available for bypassing popular mitigation solutions like Cloudflare or Incapsula test their efficiency and the company's ability to communicate tightly with the customer, since eliminating such threats is a question primarily of cooperation. PDNS/SSL-cert-scan for custom solutions dictates the necessity for L2 MPLS for enterprise customers.

Bypass and publicly available interfaces for bypassing various kinds of solutions are a serious issue and a threat to the industry. In 2017 cyber-attackers were very fast and smart, scanning and analyzing systems and then striking very hard at the most unexpected moment. Communication alone between a responsible service provider and the customer can make such a scenario impossible.

Good things are happening too; however, as always it is hard and slow to implement positive changes across the internet.

We have always said that attackers are smart and persistent; they also have many tools at their disposal. They learn DNS history, search through RIPE DB, looking glasses, announcements and paths to the target. The Times when a mitigation solution could be purchased and enabled at the beginning of the attack to reliably defend against it are gone. Nowadays we are seeing the worst case scenario more often, with businesses relocating from one datacenter to an entirely different location for mitigation purposes.

Bypasses are something that every company should be aware of since many hardware appliances and software services can be bypassed. The External IP or port you "forgot about," peripheral hardware that you were not fully aware of, these are a few of the many issues that could create moments that would cost you nerves and uptime.

Why is this happening at all? In the past, we knew for sure where "our network" was, and the exact contours of the network perimeter. In 2017 we saw a considerable change: everything is rapidly being distributed and miniaturized. In many companies, it is hard to account for all resources, activities, connections and dependencies over the network. Moreover, the possible outage of a prominent provider, like Google or Amazon could set off a damaging chain reaction for a large amount of important internet services. In the era of integration, this is a real and significant risk — we should better account for the complexity of our infrastructure.

7

Predictions fulfilled

The "I have no problem" attitude remains prevalent in many parts of the IT world. This is an illusion which we try to fight. It is a long fight.

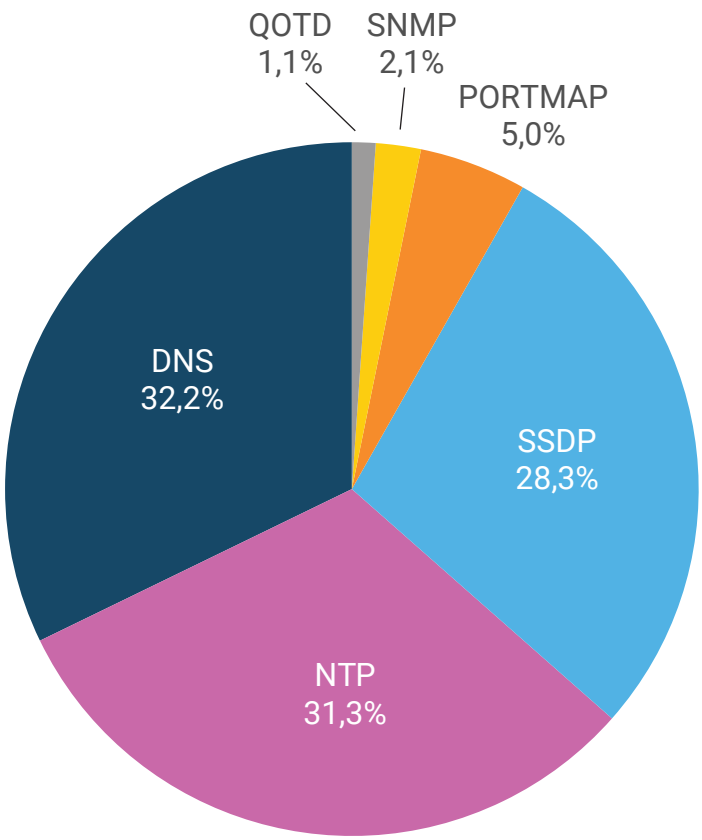
The numbers are growing: networks, autonomous systems and ISPs. With internet companies entering the networking market everything is scaling as more players take control of traffic. Of course, this means that there will be more incidents in the future since no prerequisites are created to avoid network anomalies—except for monitoring.

False positives occur when a customer reports an attack, but after some investigation, it becomes clear that no attack took place and the server experienced downtime due to other issues. Such incidents happen frequently.

Surprisingly, load tests could also become a problem since DDoS-mitigation is a very sensible system that should learn about normal user behavior as well as the attacks behavior to separate one from another. Load tests are often smarter, somewhere in between trying to find a place in the service architecture that's easy

Community awareness needs to be improved since this is a perfect and informative way for everyone to deal with what we experienced in 2017. Qrator Labs. Radar not only provides everyone with a real-time monitoring tool, but we are also active participants in the IETF community, with our latest draft on BGP roles undergoing the RFC status. Also, we are contributing to the source code of the most popular routing daemons: Quagga and Bird. We plan to add much automatization to the Radar and want to make our tools even more visual in the upcoming year.

Attacks by protocol



to exploit. When we know about such testing we could closely monitor what's going on and tune the filters, but load testing without any preliminary notion is an actual DDoS-attack that would be mitigated, and not all technicians understand that.

A standard example is auto testing that was common in 2017. To efficiently perform such tests they are most commonly whitelisted on the mitigation-service side to run uninterrupted. However, sometimes such tests could interfere with service availability,

	Average amount of IPs within 1 attack	Single attack average requests amount	Single attack average duration (minutes)
SQL Injection	26	60	37
Remote Code Execution	26	2	25
XSS	26	3	19
XXE (XML eXternal Entity)	20	8	46
NoSQL Injection	12	5	14
Path Traversal	26	3	10
Bruteforce attacks	11	93	110
Credential stuffing	25	164	327

Detailed statistics

To illustrate the typical attacks we chose the e-commerce sector data. Attacker are traditionally active here and Wallarm detects different types of attacks on various vulnerabilities vectors as well as bruteforcing everything that is possible to pluck.

Moreover, last year appeared to bring the continued logical evolution of threats to the internet and beyond. Without noteworthy DDoS-attacks, we did see remarkable ransomware spawns. There were several during the year, plus data breaches that affected entire nations. The word "privacy" itself should be redefined to include connected devices rapidly covering our planet and continuously getting hacked, used as proxies or collectors. This sounds like a dystopian fantasy.

and being whitelisted means the IP sends as many requests as it wants so there is nothing we could do. We had to deal with whitelisted attackers several times during 2017.

Compared to the extreme case of 2016 in terms of DDoS attacks and mitigation, 2017 was a peaceful year without dangerous global attacks. Several factors are behind this change, including:

— The concentrated botnet power, enabled by cameras, DVRs and routers hiding behind NATs was captured, dissolved and re-captured again dozens of times. So over time botnets disbanded in the hands of their newer owners. Competition for that power among those wanting to try some new code to see what would happen led us to very frequent low-scale attacks. But this does not mean that a new super-botnet will not start deadly attacks one day.

— IPv6 is already here on a mass scale, which means a continuous decrease of NATs covering multiple devices. Since, there are still no adequate conventional security measures, including network security, among end users we expect to see a lot more tools drawn into botnets. TVs, smartphones, almost every device connected to the internet.

— The prosecution of the Mirai creators provided a dramatic image of young men who did wrong and it all started with game servers. Any service with at

least few dollars of revenue could attract curious individuals looking to cause some trouble, and it is easy to be tempted towards the wrong path. That is why Mirai made such enormous bandwidth attacks—just to prove someone wrong. The commercial DDoS-attack market prefers L7-attacks, as they tend to be more cost and time efficient.

Older vulnerabilities are being patched, which should not go unappreciated. In 2016 we saw numerous Wordpress attacks—in 2017 these Pingback attacks are no longer such an issue as the number of vulnerable hosts decreased.

DDoS-mitigation companies could do more harm than good, ruining connections for groups of users in the name of security and profit. The greater the distance between the user and the server—the worse it gets. Politics and policies lead to diminished availability of specific resources for specific users, and the list of unavailable resources grows quickly. This leads to the segregated Internet, where access to resources is not universal and equal for everyone, representing an unfortunate tendency.

Network transparency must be a sacred cow. By this engineers usually mean perfectly equal network level processing, without any priorities. Unfortunately, traffic shaping is a reality that is rendering the Internet hardly transparent.

We are disappointed to see undisclosed practices that are inconsistent with predictability and transparency. If specific flavors of traffic, like video, or voice, receive priority it should be done according to the RFC, which is often not the case.

Additionally, ISPs doing business connecting new customers have lots of equipment on the periphery of their networks: DPIs, firewalls, etc. Such hardware could inject customized advertising, scrub and analyze traffic and contain vulnerabilities. As ISPs tend to add more value-added services we do not expect the current situation to change in the foreseeable future.

Networks belong mostly to private commercial interests, and strangely it is believed that they should serve everyone equally. Of course, in real life, an ISP would give preference to the higher margin customer over others.

Black market

End-users have always suffered and will likely suffer more in the future. It was revealed last year that the most

Lots of people and organizations: surveillance, state-affiliated or sponsored, enforcement agencies, individual professionals and just curious kids—everyone is in favor. A grey market has already formed with exploits, botnets and other "industries.". In 2017, we saw many malware archives and epidemics all over the world along with extortion software.

popular OS in the world is Minix, which is open-sourced and installed at -3 level of Intel integrated circuits to manage all system resources. A hack activated and spread via network level global infrastructure would be a disaster impacting an enormous number of systems. There already are vulnerabilities, and there could be many other possibilities, so this is a genie in a bottle and the bottle is already opened.

Malware economy is not new but it continues growing. It follows its own laws. Recently RAND Corporation released an important report on zero-day vulnerabilities saying that this market is smaller than the defense industry and shrinking. However, this does not mean that the shadow economy is shrinking—it will adapt by finding new income sources. People who do this regularly evidently like it, and there's no indication of any decline. They are just shifting their focus.

The CDN dominance

That is not about CDN itself—it is about internet consumption and the last-mile connection. If we look at CDN prices and profits and ISP prices and profits, it is clear that they are dropping faster than the overall connection rate is growing, for any given country. We now have more than 4 billion people online globally, and in most developed and developing countries there's no lack of internet connection. People are

Content and transit models are undergoing massive change right now. Moreover, at the end of 2017, we can imagine a situation where ISPs pay users for the transit of their data. CDNs and ISPs are quite similar, actually, so maybe a future with "delivery networks" is possible, especially if content-providers (meaning services and networks accumulating user data) begin selling internet access services.

trapped without communications in places that lack classic infrastructure: roads, cables. Providing them with a connection is a challenge, and there are groups of people and companies trying to offer good solutions in such areas.

CDNs are easier to deploy and manage in terms of DDoS-mitigation because when they sell mitigation, they think of it as a "side-service". This approach hides serious risks since there is no guarantee that the CDN could survive a severe DDoS-attack. On a small scale—absolutely, but in 2017 we are dealing with fast and merciless smart L7 DDoS, which could not be "cached" in the common sense. At some point, you would see the captcha.

In 2017 nobody argues that cloud networks including the CDN service are the future in terms of connectivity. They have almost arrived because the market demands large scale solutions, which means that you also need DNS, BGP and DDoS-mitigation infrastructure. However, the initial architecture could differ from one network to another, from BGP balancing to DNS, CDN/ADN and everything else.

8

Predictions for 2018

When we made our predictions about 2017 a year ago, we assumed that the entire industry would maintain the momentum it had, specifically regarding DDoS-attacks. Last year the industry exploded with other things—blockchain, crypto, ransomware, leaks of private information and so forth.

Infosecurity incidents are perceived as a threat worth attention though. The Uber leak of personal data, the Equifax breach, WannaCrypt, and NotPetya—everything happened last year and drew attention to security as a concept.

Security processes are slightly incompatible with current tendencies towards being flexible, continuous and microservice-oriented. Security still is a peripheral priority, delivered somehow and often not thought of during product development.

Even security solutions evolve. Security is now build upon threats as they are perceived—firewalls, DDoS-mitigation, Data Leak/Loss Prevention (DLP) systems. However, the threat itself evolves as well. The zero-day market is dying because there are so few researchers, brokers and companies willing to pay for those solutions. Greyhats are working on bug-bounty grounds; researchers work with companies directly. Hacking attacks are still combined with DDoS-attacks since it is easier to take what is targeted when the victim is regaining consciousness. Zery-days are much the same, and vulnerabilities too because any one alone might not do any harm, but a combination of 2 or 4 would. If attackers have any understanding of the internal processes of their targets they would find a specific combination of needed tools will be most effective.

A recent but persistent market trend is the use of Artificial Intelligence (AI), although in some cases the fashionable term is hiding the inability of underlying products to perform basic tasks in a more conventional fashion. AI can help with many tasks, such as anomaly detection as implemented by Wallarm or automation, but it does not yet work as a primary decision maker. DLP relying on an AI does not work. AI at Security Operations Centers (SOC) could be applicable, but only after initial training and under supervision. AI is much more efficient on the attack in terms of automatization, which could soon be an issue for the whole industry.

All this is a natural answer to increased levels of technological complexity. For growing businesses today, it is a real challenge to grow their networks rationally and economically. Automatization is very important, and it is often better to perform a task in a prepared auto-mode than manually with constant, possibly unnecessary adjustments to sensitive controls on expensive equipment.

Further development of the DDoS services—stressers and booters, malefactor services are getting closer to average users, not to mention the improving user-friendliness. Test attacks are often free in order to demonstrate the ability to stress the given website.

9 Outro

We have seen how fast, in just the past year, the whole world transitioned from one state to another. Extortion emails simply threatening DDoS-attacks mass emailed to thousands of companies can provoke panic. Such a state neither helps in protecting the resource, nor allows for long-term planning. Threats should be addressed in advance with preparation.

Every service has certain components that are essential to its success. We have chosen few stories to illustrate the breadth of questions an IT company has to solve in order to deliver the service.

The main purpose of building a DDoS-attack mitigation solution is to establish a defense that is cheaper than the offense, taking the financial advantage from the attackers. And this is a very difficult task because of two strong factors:

- **A Reckless approach to main infosecurity issues and threats**
- **B Threatened infosecurity market, news affecting companies lives**

Hardware and software of 2017

We like the situation we find ourselves in right now because the most positive aspect of the market is the broad choice of processors used within certain appliances, like switches. As recently as 2016 the selection was limited to Mellanox and Broadcom. We needed more alternatives for some time and 2017 brought new options as competition in 100G-400G switch chips heated up. Apart from Broadcom and Mellanox we see promising products from Cavium, Barefoot, Innovium, and overall the market is very hot. In 2017 we can get great hardware at modest prices—the result of competition in this market.

AMD unveiled a great new CPU core this year, but we have not tested it yet. In general Intel CPUs still seem more efficient, but such competition leads to lower prices in the long term. Server Skylakes CPUs have been absent for quite a long time, but finally, Intel introduced them. The multicore CPU with 6 memory channels and, critically, upgraded L2-L3 caches is a dramatic improvement. NVRAM is also a fast-evolving technology that we are following closely because storage working at memory speed could be highly beneficial for some tasks.

eXpress Data Path (XDP) is marching across the Linux network community, allowing traffic management and control on a low level, which is more efficient. In 2017 we see XDP upstreaming Linux core updates, most hardware, and software vendors are already supporting this technology. This is good news. XDP offers increased performance on the same hardware, optimized for your needs.

Switchdev is also a great solution—an operating system for network switches. Vendors finally began to support it in 2017, and we expect tremendous further development.

These developments mean just one thing—

switchdev.txt
GITHUB

that we could untangle our products and services from proprietary operating systems. This new possibility, coupled with significantly more powerful CPUs gives Qrator Labs broader opportunities in building DDoS-mitigation and lower operational costs.

100 Gbps is great news for our company. In 2018 we expect to use such connections at more of our points of presence. Controlling all the available modernization options is a big challenge these days, in order to choose what's most efficient and to deploy it on time. 10x growth of the network and the network capabilities is highly anticipated by Qrator Labs engineers, as they are eager to test the new environment and make it work.

In 2017 a statement that ISPs can quickly provide 100 Gbps interfaces proved itself correct. Qrator Labs is upgrading connections to new interfaces wherever possible, not only because of economic efficiency, but also because of the control gained over all that bandwidth. Before, we had to rely on how specific operators distributed traffic among 10 Gbps channels. Now in most situations we control the entire flow which is much better for DDoS-mitigation purposes, as well as being better in general for more prominent clients.

What we need is a new transfer protocol, fully enabling mobile networks and devices. If the protocol bears the ID of the crypto entity we are communicating with—application, smartphone, user, no matter which

Attacks are becoming increasingly complicated. Even worse, high-profile web services, the blue chips, are experiencing attacks that cannot be immediately repelled. Separate client analytics show exceedingly strong intent to bring down targeted resources.

if it is approved, then filtration based on the cookie is possible on a transfer level. Because the mobile network is a pain—when your station changes you could abuse TCP-IP level of communication as well as the interconnecting application layer.

Customer orientation

Another issue of renewed importance is that every client should be checked and double checked. On the market of DDoS-mitigation, where Qrator Labs' reputation is the major selling point it is in our best interest to make sure that there are no holes anywhere

Integrating with a customer supporting his distributed network is always tricky. The more complex the infrastructure is, the more time and effort it takes to thoroughly plan the appropriate steps and perform the necessary integration and tests. Sometimes such extensive services require fast changes which could always be problematic, especially when we operate under an SLA and the SLA does not permit unplanned changes.

in the client defense structure. Detailed connection guides, security guidelines, and how-to lists do not work with dozens of engineers in a big company communicating with each other and the mitigation service provider. We have reached the point, where a single move could create such an opening that the service instantly becomes totally insecure and could be disrupted with ease. So instead of updating public instructions, we reviewed our internal procedures to upgrade our methods and best practices to enable us to closely monitor the needs and requests of our customers. Surprisingly, we frequently receive specific requests from customers, the fulfillment of which would expose them to DDoS-attacks. Requests from our customers cover the full range of complexity, some could be answered instantly, and others need time to implement. We always tell customers that they should not hesitate to contact us and, more importantly, they should not make any moves until they get individual help from our engineers. Being under attack or just tuning the service can be tremendously stressful and lethal mistakes can be made, so it is essential not to shoot oneself in the foot when actually trying to run faster.

Each and every business owner or CTO/CISO should realize and remember that haste will not improve mitigation, quite the opposite actually. Moreover, in DDoS-mitigation there are a lot of hard knocks that could prove painful, especially when we talk about HTTPS-traffic processing.

Small companies often act in such a self-destructive manner, where there is no inner voice saying: "What are you doing?!" and actions are taken that put the whole business on the edge of survival.

So customer diligence should constantly be in process by the company, like a steady part of the workflow. Since the DDoS-mitigation solution is quite

HOW TO MEASURE THE NOC EFFECTIVENESS?

15 MINUTES

TIME TO REACT TO A REQUEST IN 2017

complicated and we integrate deeply with our customers, they do not always understand what is happening between us, how everything is working together or if it is working at all? Until an attack, there's no difference, so it is not possible to "feel" the mitigation, though it costs significant money and we have to confirm several times that everything is ok. Otherwise, there could be horrible consequences for the customer and sometimes for us as the filtrating network.

Documentation is an essential part of the complex system. The absence of proper documentation is a huge problem for many companies with required resources. Documentation should also be understandable, and maybe even a little bit entertaining, or no one would read it, even when necessary to find urgent guidance.

Additional infrastructure checklist:

— A DDoS always seeks to take down the targeted web-resource rendering it unavailable, unresponsive, or unreachable by exhausting the limited resources of a given network-connected entity, which may or may not be the actual target
— Latest updates and Security Advisory recommendations for every piece of software and hardware installed
— Virtual Machines and containers (actually working enabled for restart on failure, copied and backed up)
— Query/response load and debugging front-end testing (like HTTP 200 response on a GET / query and not something else)
— DNS
— BGP
— Channels/uplinks (connection parameters for internet providers or transit operators)
— Database: proper access and security policies
— Network equipment and software installed or used, including third-party cloud services and applications (NAT, connection tracking, firewalls, IDS/IPS, WAF, CDN)

Any finite resource can be exhausted, regardless of whether it is money, time, or people. All such attacks could be considered DDoS and it is necessary to know your disposition of such resources and how they could be additionally protected or reserved. In the world of business, financial stress is often the most visible, that is why you should always think of risks of collateral damage from attacks on neighbors/ business partners, especially in terms of your systems.

Global internet infrastructure is hardware deciding how to process packets.

Case Study **Lazada**

The moment we chose Qrator Labs as the DDoS-mitigation provider, we were already protected. With our previous solution we felt unprotected because of their slow reaction time to attacks and their scrubbing quality, or poor attack recognition, which generated too many false positives. Communication with their technical support was slow and often ineffective, we could not get answers to our questions.

Eventually, we realized this had to stop, so we began to search for a more appropriate solution. We had already heard of Qrator Labs, and its founder Alexander Lyamin, so we decided to consider the Qrator mitigation network. After our initial tests and market analysis, it was clear that the offer from Qrator had the best price/quality ratio.

Lazada is the fastest growing marketplace in South-East Asia and it must always be available for both customers and merchants. “Availability” here means not only that the website itself is accessible, but that it is reached as quickly and seamlessly as possible.

Paths of escalation during attacks are critical; sometimes there is no other way than to call the CTO… however, we never did.

Based on 16 months of experience with Qrator Labs DDoS mitigation service we can state that proficiency of their technical support differentiates the company from any other providers on the market. The combination of this high quality with their speed in processing technical questions, issues and requests makes the Qrator Labs network operation center and their tech support team one of the best in IT security. Since attacks and incidents are unpredictable, it is vital that when they happen, communication remains precise, fast and professional in order to satisfy the customer.

We do not need to mention the quality of Qrator’s scrubbing and attack mitigation since its high quality is taken for granted—a company with our size and technical requirements cannot afford to settle for providers that are not fully open and do not have our total confidence.

We experience on average one minor attack every one to two weeks. Every two to three months, we experience serious reinforced attempts to DDoS-attack our system. Once or twice in a year, we see extreme incidents, even targeting entire network, to which we must respond immediately and aggressively to cure together with Qrator Labs engineers. Sooner or later, attacks become routine, something that happens and we know that, but we would see the details in the next day’s report.

We measured the latency of our network and the speed with which our average user sees a page delivered in the region we operate, and Qrator Labs is improving those parameters slightly. There’s not much room for improvement though, and a positive change by several milliseconds is a lot in this case.

After one year of working together we asked Qrator Network to protect our DNS too. We had some specific feature requests that Qrator Labs quickly implemented, within weeks, which is fantastic. It can be difficult of require such customized solutions but when the feature is delivered exactly as hoped - it feels great.

Working with such a company represents an exciting opportunity for us.

Case Study **SDVentures**

SOCIAL DISCOVERY VENTURES

This comparison was made by SDVentures at the end of 2017 and original methodology was the following:

> With the help of websitepulse.com tools, from 3 locations within mainland China (the first column) data centers we made 5 measurements to the specific destinations (second row). We discarded 1 best and 1 worst results, averaging 3 results left.*

The whole point of this case is about the professional quantitative approach in benchmarking new products and services, as well as comparing services regarding specific requirements and use cases. The methodology could be improved continuously, as well as questioned, however, since this is not something of Qrator Labs production we have decided to take these measurements into our 2017 annual report on the state of cybersecurity.

Such tests illustrate the correct and practical approach for obtaining benchmark metrics in the form of business-specific performance indicators. Such activity in benchmarking cloud services shows that the level of technical proficiency at the company, running those tests, is high. Not believing marketing materials and conducting own research is a good thing, as we have said multiple times earlier and the main reason for open-sourcing our set of the RIPE Atlas tools to simplify such activities for interested parties.

Being able to formalize such parameters you want to test and reason them is very important and not comfortable in most situations. Measuring incorrect parameters would not help you understand what product or service is better suits your business case. Mainland China is also a highly specific case for measuring, because of the well-known Great Firewall and how it influences standard packet transmission and processing.

Measurement as the key to transparency
QRATOR LABS. RADAR

Measurement tools
GITHUB

	Akamai	Incapsula	Qrator	Akamai	Incapsula	Qrator	Akamai	Incapsula	Qrator
	/texts/forms/purchase/purchase			/users?filter=photos&gender=...			/users/429790031/photos/06b15		
Beijing, China	4.909	2.370	0.910	3.083	0.502	1.133	3.955	0.612	1.135
Shanghai, China	1.523	0.546	0.400	2.711	0.692	0.321	2.640	0.954	0.320
Guangzhou, China	2.986	1.009	0.370	3.002	1.044	0.452	3.374	1.049	0.519

* Given methodology and results originate from our customer and should be considered with precaution.

About companies

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.

qrator.net

press@qrator.net

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.

wallarm.com

press@wallarm.com