QRATOR LABS

wallarm

Russian and Worldwide Internet Security Trends 2015

Main threats:

DDoS attacks and web application hacking

This report contains the main corporate site availability and security trends and issues of 2015 related to DDoS and “hacking” threats. It is prepared by Qrator Labs and Wallarm specialists and based on industry situation monitoring (in Russia and worldwide), and on statistics collected from their customers in 2015. In addition, this report includes data from independent company research conducted on behalf of Qrator Labs.

Significant numbers of Qrator Labs and Wallarm customer companies represent different industries helping to draw a conclusion on the overall status of internet security.

The report also contains data collected from Qrator Labs’ service, Radar.Qrator.net. This is a unique global internet monitoring system; its data is accessed as a service by internet providers and telecom specialists. Qrator Labs and Wallarm experts are permanent participants of industry international conferences, their presentations are highly regarded by IT and telecommunications professionals from around the world.

KEY OBSERVATIONS OF 2015

1. As the complexity of attacks increases, hackers combine various approaches by responding simultaneously to DDoS attacks and attacks against application vulnerabilities.

The reduction of DDoS attack peak rates became the main observation of 2015, which does not sound optimistic, however, as it is compensated by their increasing complexity.
Previously the adversaries mostly relied upon a single DDoS type, while today the attacks acquired a multivector nature (i.e. can be targeted at several network layers or infrastructure elements), and are becoming more complex.

Hackers complicate their attacks further by combining DDoS with “hacking”, i.e. attacks against application vulnerabilities. In 84% of cases a DDoS attack is accompanied by a site hacking attempt. Thus, today the security solutions focused on DDoS protection alone prove to be insufficient in providing internet resource availability.
Nevertheless, the companies with an integrated approach to the organization of an increased complexity attack mitigating system are able to successfully mitigate such risks (ref. the case of Qiwi payment service in the “Combined attacks” paragraph below).

2. Implementation simplicity and minimum costs of attacks.

It has never been cheaper to organize a DDoS attack – the cost of this procedure starts at $5 per hour. As the result, the average attack count per site doubled in 2015 in comparison to 2014. The adversaries proactively utilize cloud service providers for swift a cquisition of resources, particularly tollfree, by using bonus or trial programs.
The situation with hacker attacks is similar. Due to the availability of tools for search and exploitation of vulnerabilities, a successful attack often does not require any major expertise: instead of professional hackers, the attacks are more often carried out by less qualified ones who search and exploit known vulnerabilities utilizing pre-made tools, and relying upon instructional articles and videos.

3. Application layer (L7) attacks became the main challenge in terms of DDoS protection.

In 2015 application layer (L7) attacks often accompanying DDoS attacks against the channel layer (L2) became more frequent. Protection from the application layer DDoS attacks is the most difficult case, requiring maximum expertise and quick reaction to the attack vector alteration. Furthermore, hackers utilize smart automated tools that deny the possibility of single specialist counteraction on part of the protection. Today one can say that only machine learning algorithm based systems can efficiently mitigate DDoS. Human operator controlled systems fail to cope with modern multivector attacks in real time without considerable interruptions in customer traffic service.

4. The most common vector of hacker attacks aimed at site hacking is still SQL injection type vulnerabilities. Mass traversal attacks became the new challenge.

The most popular attacks are still SQL injection type vulnerability exploits (37.75% of total attacks), when a particularly formed query allows for the execution of a custom query to an application database. They are easy to implement with the aid of automated tools and grant an adversary direct access to a resource database. The protective solutions are more often avoided by means of various types of malicious query obfuscation (cloaking) which proves efficient against WAFs that ignore application specific features and structure.

Last year the number of traversal attacks, including password traverse, increased significantly (21.85%). In Russia this particularly affected internet retailers with a massive number of cases where adversaries gained access to accounts by using username/password databases leaked from other sources.

5. Various groups utilize mass internet scanning techniques.

The capabilities of mass scanning of the whole internet is not limited to Google and other search engine giants anymore: now it can be done for various purposes by different groups of people. The adversaries try to find web resources, routers, and IoT devices with known vulnerabilities for swift and automated control capturing. These resources are further proactively utilized for the purposes of powerful DDoS attack accomplishment, anonymisation, cryptocurrency mining, etc. “The main conclusion of 2015 is that the industry came to an understanding – today the protection with individual means became impossible. It is necessary to use continuously updating professional solutions that utilize machine learning algorithms in order to successfully mitigate complex integrated DDoS attacks and hacking”, says Alexandr Lyamin, the head of Qrator Labs.

> “The main conclusion of 2015 is that the industry came to an understanding – today the protection by individual means became impossible. It is necessary to use continuously updating professional solutions that utilize machine learning algorithms in order to successfully mitigate complex integrated DDoS attacks and hacking”

CHAPTER I. DDOS ATTACK ANALYSIS

DDoS attacks are still used as an instrument of unfair competition. They become more popular with each passing year. 2015 was not an exception – the Qrator Labs forecast, pessimistic as it had been, was surpassed. The company had predicted a 25% increase in the number of attacks, while its actual indicator grew by 100%.

+ 100% IN ONE YEAR

THE INCREASE IN AVERAGE NUMBER OF ATTACKS PER SITE DOUBLED

It has never been cheaper to organize a DDoS – today the cost of this procedure starts at $5 per hour. This is an approximate cost of the infrastructure lease required to organize an attack.

As it has been before, the companies from ecommerce, banks, and social networks remain the primary targets for the adversaries. In addition, travel companies and real estate agencies were among the most frequent targets in 2015, which could also be connected with political reasons and economical pressures.

According to the research data conducted by 42Future analytic agency on behalf of Qrator Labs at the end of 2015, 25% of the largest retailers encountered DDoS attacks over the past year. The number of retailer site attacks escalated by approximate 70% as compared to 2014.

80% of the respondents have reported that they believe the attacks were primarily ordered by their competition. The second reason for the attacks was blackmail, as it has been stated by 45% of the respondents.

AVERAGE NUMBER OF DDOS ATTACKS PER CUSTOMER PER MONTH FOR 2014 – 2015

	Amplified DDoS	All DDoS
Online stores	25%	70%
Social networks	73%	159%
Coupons	-25%	-10%
Forex	-53%	-62%
Payment service	74%	37%
Games	42%	110%
Trading platforms	-15%	-18%
Banks	121%	61%
Mass media	-29%	17%
Content aggregators	-43%	-28%

	Amplified DDoS	All DDoS
Promo sites:		
Real estate agencies	113%	144%
Advertising agencies	-40%	-16%
Micro financing	-30%	-36%
Travel companies	-1%	145%
Taxi	116%	108%
Medicine	-20%	-54%
The rest of promo sites	-58%	-34%

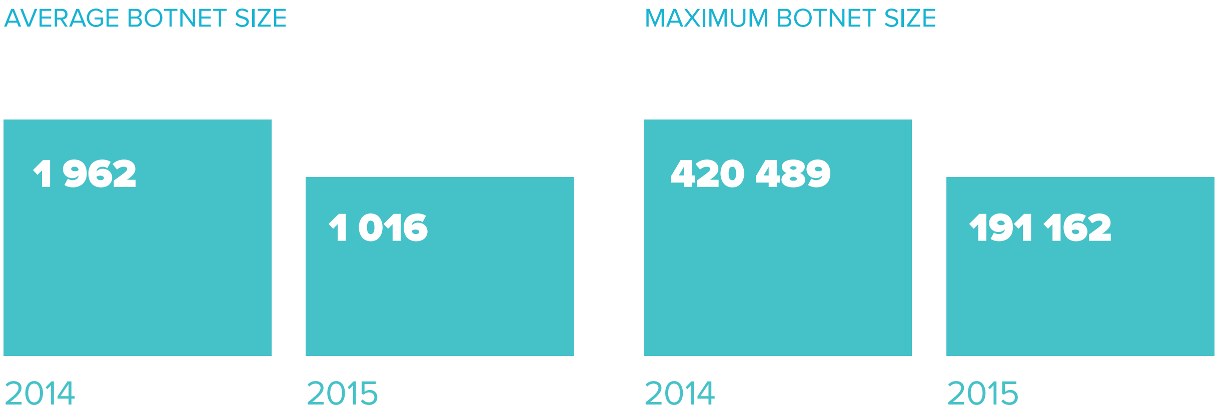
TREND 1. AMPLIFICATION TYPE ATTACKS

In 2015 the Armada Collective made themselves known by blackmailing companies and demanding a bitcoin ransom under the threat of a DDoS attack. Plenty of such incidents took place around the world, and they got wide press coverage. The adversaries avoided seizure, and the group remained active until December 2015.
Although it has not become clear whether it was the same group of adversaries that took part in all known cases of blackmailing, threatening letters were often received by several companies in different countries at the same time.

It is highly probable that there appeared the successors of the first Armada group acting by the same scenario and using the same name. Armada became a phenomenon.
It means that even if a group of cyber criminals is taken into custody, the occurrence and the threat they have created will not disappear.
The scheme works: there are companies that agree to pay the blackmailers. Some of the cases were reported by the press, but a lot of them remained behind the scenes, although they are known in the professional circles.

Unfortunately, the risks cannot be eliminated by paying the ransom which is proved by the known cases of site attacks that continued even after reception of the money.
In addition, the companies that agreed to pay the blackmailers virtually invested in their infrastructure used for further attacks. That means they directly support the adversary's business.
The only possibility to mitigate such threats is to utilize specifically developed and continuously upgraded tools as the adversary techniques constantly evolve as well.

Armada used attacks with an amplification technique (Amplification type attacks), which vividly illustrates the trend of 2015. This specific type of attacks became the most widespread occurrence in 2014 and the trend continued in 2015. Amplification type attacks are accomplished the following way: a query is sent to a vulnerable server which replicates the query and sends its multiple copies to a web resource of a victim. DNS-, NTP-, SSDP-servers
and other servers can be exploited as involuntary participants of such attacks.



This information graphic demonstrates that in 2015 the botnet size involved in DDoS attacks decreased. At the same time, the number of spoof attacks, which include Amplification type attacks, increased.

In Amplification type attacks botnets are seldom used for generation of the first wave of junk traffic. Either leased servers or hacked servers are used for this purpose. Even if lease is the case, it will not cost much to organize an attack, for it is enough for an adversary to generate queries at several Gbps rate and direct them to a vulnerable server, which in turn will increase this rate by a huge ratio.

100
AVERAGE MULTIPLIER RATIO
IN AMPLIFICATION TYPE ATTACKS

30-40 GBPS
MINIMUM AMPLIFICATION TYPE
ATTACK RATE IN 2015

It is already impossible to counteract such attacks manually as they are too numerous and too expensive to counteract. The actual costs the adversaries i ncur for the infrastructure required to organize an attack are a few dozen times lower than those of a victim company trying to mitigate such an attack individually.

TREND 2. COMBINED ATTACKS

L2 and L7: channel and application layers

The most popular scenario the companies used for DDoS protection in 2013 – 2014 was as follows:

- for a channel layer attack (when channel capacity is being depleted with junk traffic) the companies relied on protection granted by the provider;
- for infrastructure attacks they used “selfwritten” or local solutions implemented on their own servers.

The attempts to independently mitigate the channel layer (L2) attacks gradually recede into the past. In order to accomplish that it is necessary to organize and maintain an expensive communication channel and a distributed infrastructure (in several datacenters).
Therefore the companies prefer to rely on their internet providers or start using professional cloudbased counteraction tools, such as Qrator. But is it worth to completely rely on an internet provider? In Summer 2015 an incident occurred that resulted in the disconnection of five US cities from the internet. The server was subjected to DDoS attack by a specific IP, which easily “jammed” the local internet provider channel supplying access to residents and companies in several metropolitan areas.

“I am sure there will be plenty of such stories to hear. Attacks are picking up pace and becoming more and more intricate. Small internet providers operating on “the last mile” are often incapable to mitigate even a secondrate attack. In this case five cities were serviced through only a 10 Gbps capacity communication channel. That means the capacity greatly smaller than a typical DDoS attack of 2015 was enough to completely jam the channel. In addition, the network was organized in violation of minimum fault tolerance standards, thus the technical support specialists were unable to reach their main provider by phone so that the latter blocked the attacked IP, as the technical support telephony was deployed on the same channel”, comments Alexandr Lyamin, the head of Qrator Labs.

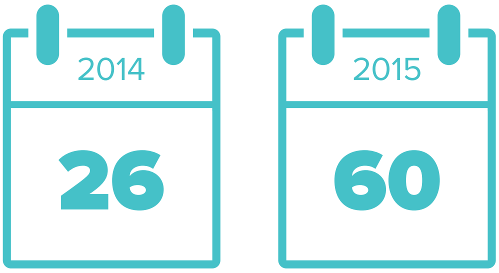
The majority of large and most advanced companies have also ceased to experiment with selfwritten tools and locally installed solutions for mitigation of application layer (L7) attacks. The attacks are becoming too numerous and the protection tools that require manual interaction are ineffective. The DDoS mitigation should occur automatically.

QIWI payment service represents a good example of how to organize an effective increasing complexity attack mitigation system. QIWI internet resources were attacked 25 times in 2015 and the maximum attack rate reached 16 Gbps. Nearly all the attacks were aimed at HTTPS services that provided encrypted transactions for the service's customers.

15% of attacks were accompanied by hacking attempts.

The company uses Qrator's traffic filtering network and WAF hacking protection from Wallarm. QIWI specialists decided a gainst building a selfsustained mitigation system. As Kirill Yermakov, CISO of QIWI explained:

"When millions of transactions pass through the payment system each day, the availability of resources becomes critical for business. The reality is that today several hundred gigabits per second attacks have become a normal occurrence, and correct tools are required for DDoS protection. Qrator Labs became a reliable partner that helped to provide the business with the required SLA and showed flexibility working with our complicated infrastructure. We use Wallarm separately to protect web applications and our multiple API. We are especially pleased that we were able to integrate both solutions with our incident response center and monitoring system."



AVERAGE NUMBER OF DDOS ATTACKS
26 60 MITIGATED BY QRATOR LABS NETWORK
PER DAY:

Utilization of reflectors, i.e. servers with "holes" in protection, which multiply traffic and direct it to a victim's site as absolutely correct application queries, presents a new possibility for multiple times increase in arm of L7 attack.

In 2015 Qrator Labs observed a great number of L7 attacks based on WordPress Pingback vulnerability exploits. There are hundreds of thousands of servers with this "hole" across the internet, which can potentially become fake query reflectors to victim's web applications.

At the end of December an attack was l aunched on a major Russian transportation company with participation of over 3.5 thousand WordPress based servers. They generated malicious traffic with the peak rate of 7.5 Gbps.

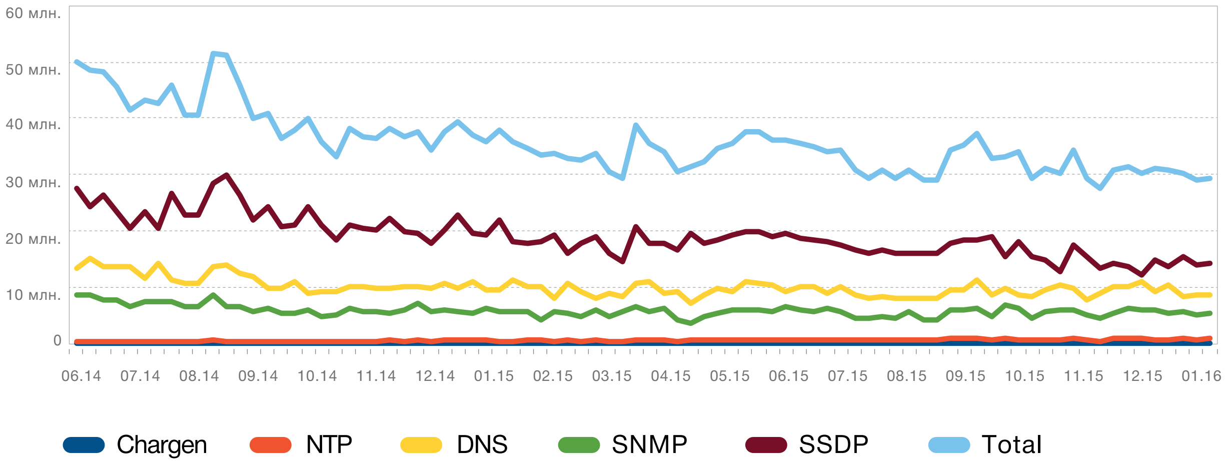
L7 attacks are cheap and easy to organize, and new ways to increase their "arm" have appeared. The protection from L7 by means of simple "homemade" tools became impossible. In this case "selftreatment" is expensive and inefficient.

More and more web resources use the protected HTTPS protocol which provides traffic encryption. This is an effective tool to protect user data from theft, but in case of attack an HTTPS based L7 server encrypts all the queries to applications including those coming from bots. In L7 a bot can only be identified by its behavior. This means that DDoS mitigation tools able to operate with encrypted traffic should be used for this case. At the same time the protection providers are often required to decline using internet resource encryption keys.

Combination of amplifiers and various layer attacks

According to statistics collected in 2015, the amplifier quantity slowly decreases. But their approximate number rests at 30 million. This means the specified attack type will still be used for a long time. In addition, new amplifiers h ave appeared that may be used to exploit old protocol vulnerabilities. The fresh examples are RIP and QotD.

NUMBER OF AMPLIFIERS



A “Standard Amplification” type attack usually involves several amplifiers at once. In 2015 a new combined attack organization trend marked its presence: an amplification attack may be followed by an application attack (L7). This means the protection should cover all the layers at once.

DDoS attacks combined with hacking

Notorious press exposure of DD4BC group activities occurred in 2015. In pursuit of illicit gain the adversaries have used (and continue to do so) various means ranging from DDoS to Trojan virus distribution, hacking of web applications and smartphones. The cyber criminals have often combined DDoS attacks with hacking attacks against sites. Iincurring losses to several financial organizations around the world. The DD4BC approach that lies in various class attacks is gaining popularity and can be called an outstanding trend of 2015.

According to Wallarm, calculation an alternation of DDoS attacks with site hacking attempts is observed in 84% cases.

TREND 3. BGP INCIDENTS

The issues of the BGP routing protocol, which serves as basis for the whole internet, have been known for several years, though it has been in the last few years that the errors the protocol contains have increasingly resulted in drastically negative consequences.

Emergency situations connected with routing at the crossdomain network layer can influence a great number of hosts, networks and even global connectivity and availability in the internet.

The most typical network anomaly is route leaking or RouteLeak. The problem emerges as the result of announcing a route in the wrong direction. For example, if an AS (autonomous system, which is the main system that defines an operator as the operator) is connected to two providers and announces the prefixes of these providers (i.e. proclaims itself the source of the prefixes), the whole traffic of both providers shall flow to the network of this AS. This will most probably result in unavailability of the AS itself, as well as partial unavailability of all the networks present in this RouteLeak.

For example, in 2008 the AS36561 autonomous system related to the Pakistan national network assumed a Youtube prefix and started to deny the traffic related to this prefix. This resulted in temporary unavailability of Youtube.

Such incidents mainly occur due to carelessness on the part of administrators or petty mistakes in a network configuration. BGP vulnerabilities have not yet been are successfully capitalized on. It is difficult and expensive to organize an attack exploiting BGP errors. But the organized criminal groups (including politicized ones) acting in cyberspace have been substantially increasing their scope for the last few years. In addition, a single successful targeted attack against a large bank can compensate the whole year of its preparation.

Therefore, notorious security incidents connected with BGP issues may take place in the future.

A case of a purposeful BGP vulnerability exploit was documentedlast year. In August 2015 a cyber group named Hacking Team, which cooperates with the governments of different countries to help them fight cybercrime, initiated the hijacking of IP addresses which did not belong to them. The hackers did that in order to help the Italian police take control of several computers which were under observation during an investigation.

The adversaries may be using such methods but the victims remain unaware. The attacks organized at the routing protocol layer and the network infrastructure layer in general are quite difficult to reveal.

Such actions can be on a huge scale and result in a wide variety of consequences. BGP manipulations may allow stealing traffic or data, organizing a DDoS attack, subtly leading users to a fake site of a popular service to acquire their username and password information, etc. Another fresh example: last year a Telecom Malaysia operator redirected the whole world's Facebook traffic which they surely failed to cope with. The issue was the result of incorrectly configured routing. As the consequence the social network users were experiencing access issues for two hours.

Although unintended, Telecom Malaysia virtually accomplished Facebook DoS of prefix hijacking type – when a network service prefix of an operator starts being used in entirely different operator network. This results in confusion as a part of user queries may be directed on an incorrect route and land at a wrong server. Telecom Malaysia incorrectly announced 179,000 prefixes thus causing third layer providers to perform the wrong routing.

“In 2015 we observed network hijacking with the use of BGP route leaks as well as plenty of ordinary route leaks but we do not know for sure if they were used for criminal purposes. The risks connected with BGP vulnerabilities are quite high. This issue can be exploited for really severe attacks including their application as a cyber weapon”, – says Alexandr Lyamin, the head of Qrator Labs.

According to the observations of Qrator.Radar (unique, in a class by itself system of global internet monitoring, innovative cloud service for operators and telecomspecialists), the prefixes prone to route leaks count up into the tens of thousands. Meanwhile the number of prefixes noted in MOAS conflicts approached 150 thousand by the end of 2015. An MOASconflict (multiple origins AS) is announcement of the same prefixes by different sources.

51 527

UNIQUE AS PREFIXES
IN ROUTELEAK

144 424

UNIQUE PREFIXES IN MOAS
(MULTIPLE ORIGIN AS) CONFLICTS

CONCLUSION AND PREDICTIONS FOR DDOS IN 2016

L7 attacks to regain popularity

In 2015 botnet capacity decreased as the adversaries switched to Amplification type attacks. The competition for amplifiers may yet again increase by the end of 2016. In addition, with implementation of mitigation tools for this type of attacks they will be more often replaced with L7 attacks (against applications). This particular type of attacks shall be the trend in 2016. The recommendation is to prepare in advance and start using combined mitigation tools based on machine intelligence technologies provided remotely.

The increasing numbers of companies from various industries transfer their sites to the protected data transmission under HTTPS protocol. Hereupon the hackers pay more and more attention to attacks against applications operating under this protocol. The general increase in DDoS quantity and steady yearly growth in encrypted traffic (a pproximately doubled in 2015) evidence that the number of DDoS attacks against HTTPS services shall increase correspondingly.

Attacks on DNS

Qrator Labs forecast of 2014 continues to become reality – the attacks against infrastructure are still rare but their numbers grow. In particular they include attacks against DNS servers.
The situations when the network infrastructure is attacked usually have devastating consequences notable even globally. Thus, 30 November and 1 December 2015 attacks against DNS system root servers were accomplished where the adversaries succeeded in disabling part of the servers.
On 14 December 2015, the DNS servers of .tr upper layer Turkish domain stopped working.

In January 2016 similar attacks continued. This time they were aimed at DNS servers of the RIPE European registry, and some of the attacks were successful. The numbers of similar incidents related to network infrastructure attacks (against DNS servers, as well as attacks connected with BGP errors) will grow in the next few years.

BGP incidents

An increasingly relevant subject is the threat to site accessibility which originated as the result of purposeful or unintended routing errors i n BGP – the fundamental internet protocol. We predict that in 2016 (as well as in 2015) about 510% of internet access provider Autonomous Systems (AS) will have issues with accessibility of their services. That means the indicator shall not grow. Though the number of AS will increase. A number of significant BGP incidents resulting in unavailability of hundreds or even thousands of networks will also increase.

TCP incidents

The internet infrastructure is continuously being upgraded in order to support the constant growth of rates. After 10 Gbps, 100 Gbps rate is becoming the new standard. At the same time there appear issues with invented at the dawn of the internet, outdated TCP protocol that is absolutely not suited for such rates.

Lots of issues may occur in this connection, related to the possibility of packet forgery by hacking Sequence Number and Acknowledge Number fields that allow the parties exchanging packets to distinguish their TCP connections.

For example, a TCP hijacking attack becomes possible allowing an adversary to turn into a “maninthemiddle” and transmit all the packets exchanged between two hosts. Consequently the adversary will be able to examine packets, send false packets, inject a connection reset command, and so forth.

“The interest in TCP vulnerabilities are presently reemerging among the explorers. I think that notorious cases of their exploitation are soon to be observed. It might already start in 2016. – Comments Alexandr Lyamin, the head of Qrator Labs. – The issues of TCP, the fundamental protocol of the global network, are so grave that if the adversaries get down to them, the whole internet may crumble. It will affect everyone”.

IoT issues

An incipient Internet of Things or IoT world presents a severe threat. All the devices connected to the internet may become parts of adversary infrastructure and get involved in DDoS attacks.

In 2015 Qrator Labs observed multitude of attacks from botnets deployed in Android devices. The number of vulnerabilities of this and other OS discovered by the adversaries will increase, thus enlarging botnet size.

The distribution of IoT contains a threat of an even larger scale – the manufacturers of various connected devices (kettles, TV, cars, multicookers, weighing devices, “smart” sockets, etc.) are far from always concerned with providing an appropriate level of protection. Such devices often use old versions of popular operation systems (including the abovementioned Android) and do not take care of their regular updates where the known vulnerabilities are eliminated.

The premonitory symptoms of IoT issues were noted in 2015. In particular, a botnet was discovered that had been built on network routers where standard passwords remained unchanged. “One would think that the network equipment is configured by specialists and must be the last to fall under the threat of hacking. But the practice shows the contrary. What is there to discuss about the vulnerability of user devices. We expect all the smartphones with the old versions of Android to become part of at least one botnet very soon. They will be followed by all the “smart” sockets, refrigerators and other household appliances. Within two years we shall be facing botnets consisting of kettles, baby monitors and multicookers.
The Internet of Things will bring a lot of issues along with its comfort and additional capabilities. We should start preparing for this now”, says Alexandr Lyamin, the head of Qrator Labs.

The recent story which happened in California illustrates how vulnerable a completely unexpected device can be. A child complained to his parents that he heard a male voice at nights. It turned out that a hacker hijacked t he baby monitor and scared the boy by talking to him remotely.

CHAPTER II. HACKER ATTACKS AGAINST WEB RESOURCES

The threat of web application hacking remains one of the major concerns for web resources of any industry. Even a technically inexperienced person could consider himself a hacker since the hacking tools and techniques are freely available and may be easily found on practically any search engine. In 2015 this topic was marked by the following trends.

KEY OBSERVATIONS OF 2015

Alteration of DDoS attacks with site hacking attempts was observed in 84% o f cases. It is highly probable that the completed DDoS attack would be followed with a site hacking attempt or the other way around.

Mass internet scanning with the aim of finding resources with known vulnerabilities concerns any site. Thus scanning for ShellShock vulnerability, which has been discovered back in 2014 and allows for remote execution of a custom code, is still fixed for almost every Wallarm customer.

31% of sites contain critical vulnerabilities of which descriptions are publicly available. That means every third site can be hacked even by an unqualified person who spent a little time. The attack amplitude increases right after public vulnerability information appears in popular media or products (CMS, forums, etc.). This said, the time between public exploit appearance and mass scanning rarely exceeds 24 hours.

The number of attacks against cloud infrastructures increases (AWS, Azure, etc.). The adversaries make use of the most common errors in cloud service management which have not yet adopted best practices.

The most popular type of attack remains SQL injections (37.75%). The possibility of direct access to a database is often the very purpose of an attack, and relative ease of its accomplishment with the use of automated tools makes this type of attack the absolute leader.

COMBINED DDOS AND WEB APPLICATION ATTACKS

According to Wallarm’s calculations, an alternation of DDoS attacks with site hacking attempts is observed in 84% cases. This evidences the concurrence of actions and ubiquitous utilization of various attacks techniques by hackers. “It is highly probable that the finished DDoS attack will be followed with a site hacking attempt and the other way around. And a suddenly stopped DDoS attack may mean the hacking succeeded”, comments Ivan Novikov, the head of Wallarm. Thus, only the simultaneous use of multidedicated protection means (including DDoS and application attack protection, as well as BGP monitoring tools) can efficiently resist hackers.

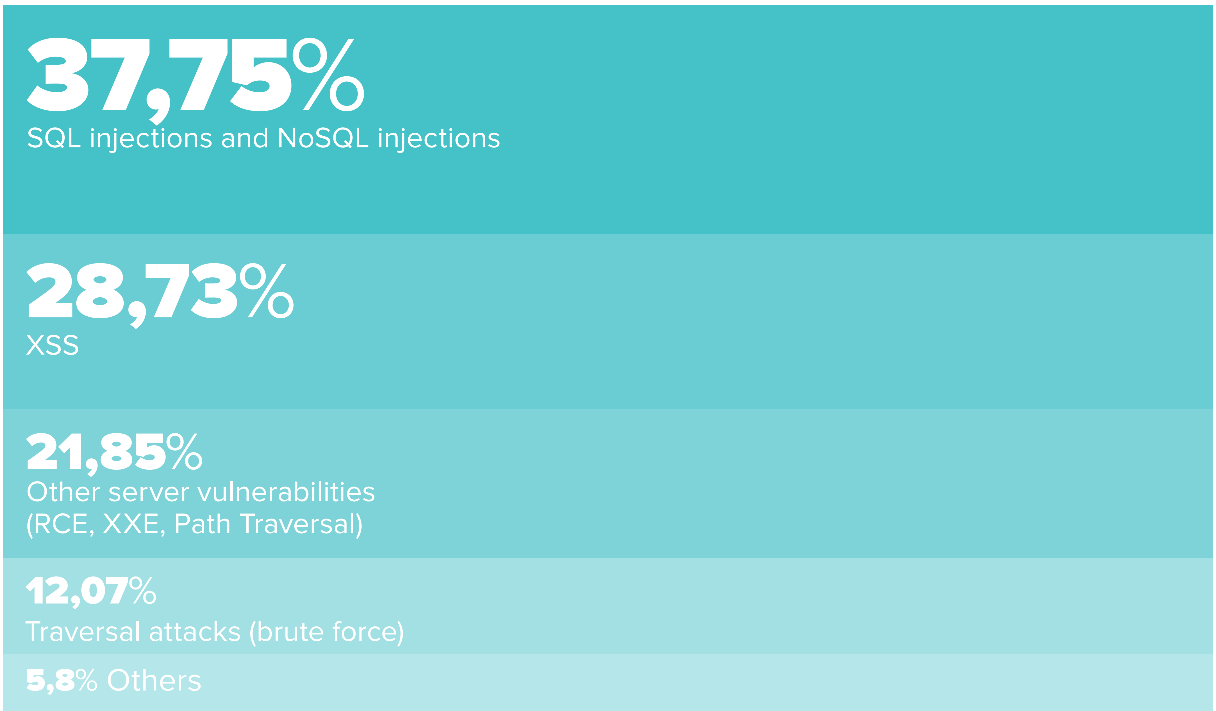
Over 30% of sites contain critical vulnerabilities of which descriptions are publicly available. That means every third site can be hacked even by an unqualified person with little effort.

This means that it is necessary to provide protection from security threats with the aid of combined integrated solutions that operate remotely, i.e. situated outside the attacked infrastructure.

WEB SITE ATTACK CHARACTERISTICS

In 2015 Wallarm recorded over 100 million attacks against their customers' web resources.

DISTRIBUTION OF ATTACKS BY TYPES OF EXPLOITED VULNERABILITIES :



SQL injection attacks comprise the largest share of malicious queries (37.75%). This is conditioned by the multitude of publicly available tools for automated web application testing for this type of vulnerability. In addition, the vulnerability risk is extremely high: a successful exploit allows the adversaries to get full access to a database.

Second place is occupied by client vulnerability attacks, socalled cross site scripting or XSS (28.73%). A successful exploit enables unauthorized access to a specific account of a victim user or their group. These vulnerabilities are much less common in web applications and considered less critical by the developers as they require interaction with the attacked user browser.

Last year was also notable for a significant increase in number of traverse attacks including brute force password guessing (21.85%). In Russia this primarily affected internet retailer sites where the adversaries were gaining access to bulk quantities of accounts by utilizing username-password bases leaked from other resources. This was given more detail in the separate internet retail security report dated December 2014.

RISK ZONES BY INDUSTRIES

The aggressiveness of the internet environment intensifies with each year. The events of mass scanning for known vulnerabilities were quite rare occasions a few years ago, though presently almost every site is surveyed each day by a check bot. Any resource, including unpopular and almost unvisited, can be hacked with automated tools.

In this case the adversaries aim at computing resources which they can subsequently use to accomplish DDoS attacks, as a proxy server, for crypto currency mining, etc.
The following resources can be distinguished in terms of attack usefulness :

1. Electronic commerce and primarily internet retailers. Fraud with bonus points, hunt for user bases.

2. Payment systems and aggregators, financial brokers and other financial establishments. Attempt to gain access to database with possibility of changing balances.

3. Gaming industry. Fraud with internal game economy, source code crash, etc.

4. Advertising networks. Fraudulent practices with internal account balances and fraud with number of displays.

5. Mass media. Disruption of accessibility and operability of resources.

In addition, web application hacking often becomes a step to access company internal infrastructure.

THE MAIN REASONS FOR WEB APPLICATION HACKING

The threshold to “join the trade” is rapidly lowering. It is often unnecessary to possess specialized knowledge to accomplish a successful attack. Once a public exploit appears for a critical vulnerability of a known product and the whole process comes down to trite specification of domain or IP address of the vulnerable resource. The minimum requirements for developers to begin working with web applications are also diminishing which is certain to affect the quality of system code.

Within the first month after connection, the Wallarm system discovers on average several vulnerabilities that could be somehow exploited by the adversaries for hacking. The most common issues that make sites easy targets for the adversaries can be summarized as follows:

1. Utilization of obsolete software (for example, WordPress or its separate plugins) and unprotected secondary resources at the network perimeter of a project, which were forgotten or neglected.

2. Basic critical vulnerabilities allowed during development or modification of software.

3. Administration errors (default passwords, careless service configuration following instructions in “made as Habre/stackoverflow” fashion.

4. Targeted PC infection of company employees who have necessary accesses (passwords to FTP, SSH, VHN, etc.), usually through phishing.

5. Accounts are published with open access by mistake (developer forums, sites like Pastebin, code repositories at GitHub, etc.).

It is worth noting that such reasons are relevant as for minor or average projects that always suffer the lack of expertise, as well as for major projects with large scale infrastructure, dynamically developing web applications and changing teams. Turbulence in human resources under conditions of crisis only contributes to this process.

FORECAST FOR 2016

1. Simplification of hacking and a continued shift in the types of people organizing attacks – from those with a professional understanding the subject matter to newcomers who search and exploit a vulnerability guided by articles and instructional videos.

2. Hacking and infection of various IoT devices. Web interfaces, API in household appliances, machines, and gadgets are built based on the same technologies and therefore suffer the same issues as multiple web resources. Mass DDoS attacks with exploitation of such devices are possible.

3. Increase in number of attacks against cloud infrastructures (AWS, Azure). Rapid cloud service development and absence of established management best practices create new opportunities for hackers.

ABOUT COMPANIES

QRATOR
LABS

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

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

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

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

www.qrator.net

wallarm

Wallarm develops web resource protection solutions that combine functions of web application firewalls (WAF) and active vulnerability scanners. The products are in demand among the internet companies with highly loaded web applications, operating in markets of ecommerce, online payments, SaaS/PaaS, Big Data, mass media and personal communications. In 2014 the company was declared the winner of the iSecurity competition held by Skolkovo Foundation among the internet security projects.

www.wallarm.com

APPENDIX

BRIEF INFORMATION ON DDOS

DDoS attack (Distributed Denial of Service) is an attack against a computing system with the aim of bringing it to failure (i.e. to the conditions when the legitimate users are unable to access the system) by depleting specific computing resources. A DDoS attack is often accomplished with great number of queries from infected computers to a server where each query is similar to those generated by legitimate users. This provokes failure of site infrastructure as it fails to support an overly excessive load compared to its normal values.

In order to generate such numbers of queries the adversaries exploit computers of internet users who remain unaware of this. The adversaries infect web servers and computers with Trojan programs thus turning them into “zombies”. Thousands of “zombies” are combined in a botnet – a network that can be controlled remotely. The largest botnet was registered in 2009; it comprised 1.9 million of computers from 77 countries. A single command sent by the hacker from any place in the world was enough to launch a DDoS attack. For this exact reason the lawenforcement bodies struggle to find perpetrators and organizers of DDoS attacks.

Qrator Labs classifies the attacks according to infrastructure elements they are aimed at:

- Channel layer [OSI Layer 2] – the attacks aimed to deplete channel capacity;
- Network infrastructure [OSI layer 3] – the attacks aimed at inactivation of network equipment (switches and routers);
- Transport layer and TCP protocol [OSI Layer 4] – various manipulations with TCP state machine: SYNflood, incorrect initiations/release of connections, buffer memory overflow;

Application [OSI Layer 7] – attacks accomplished with the use of semantically apprehended protocol constructions of the attacked internet application, for example, HTTP Flood for websites.

A separate FBS subclass (Full browser stack) of application attacks should be highlighted. Such attacks require botnets that have a fullfledged web browser with the necessary range of extensions and plugins at their disposal. Such attacks are guaranteed to overcome solutions that utilize “puzzleverifiers” for a customer – from simple HTTPredirects to less trivial verifiers that use JS/AdobeFlash or Quicktime.

TABLE OF CONTENTS