Distributed Denial-of-service attacks, The cyber-pop-up

- The DDoS attacks have increased their complexity by increasing the use of more than two vectors in cyber attacks.

- The new tactic of attack "Pulse" has enhanced the accuracy and intensity of the attacks: the largest in the second quarter of 2017 reached a peak of more than 350 Gbps and reached its peak in 190 Mpps.

- Spain was the third largest country attacked (2.1%), only behind the United States and the United Kingdom.

The second quarter of the year 2017 has been marked by multiple DDoS attacks called "Pulse", according to a study by Imperva. The new tactic allows a cyber criminal to specify multiple objectives alternating bursts of high volume and intensity with intermittent.

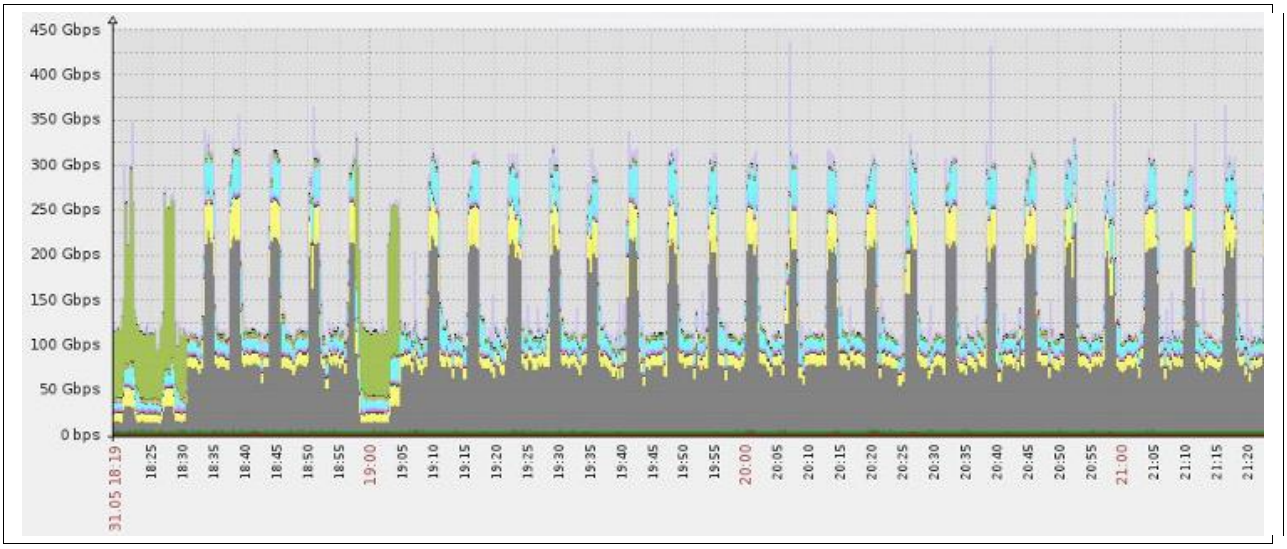
In an attack "pulse wave" run the denial of service (DDoS) through waves of pulses, they are attacks that start from scratch and achieve a high level of intensity in a short period of time, then stop completely and start the process again during continuous cycles that are activated in short intervals of time. Some mitigation solutions are struggling to cope with the attacks "pulse", Imperva has detected this new method of attack, and has mitigated with success.

More than six out of every ten attacks originate in China. While the country most affected by these attacks remains the US, list in which Spain occupies the third place.

Although the attacks in network layer and application layer have fallen in the previous quarter, the peculiarity lies in the fact that the attacks have reaching records of repetition and intensity never before recorded.

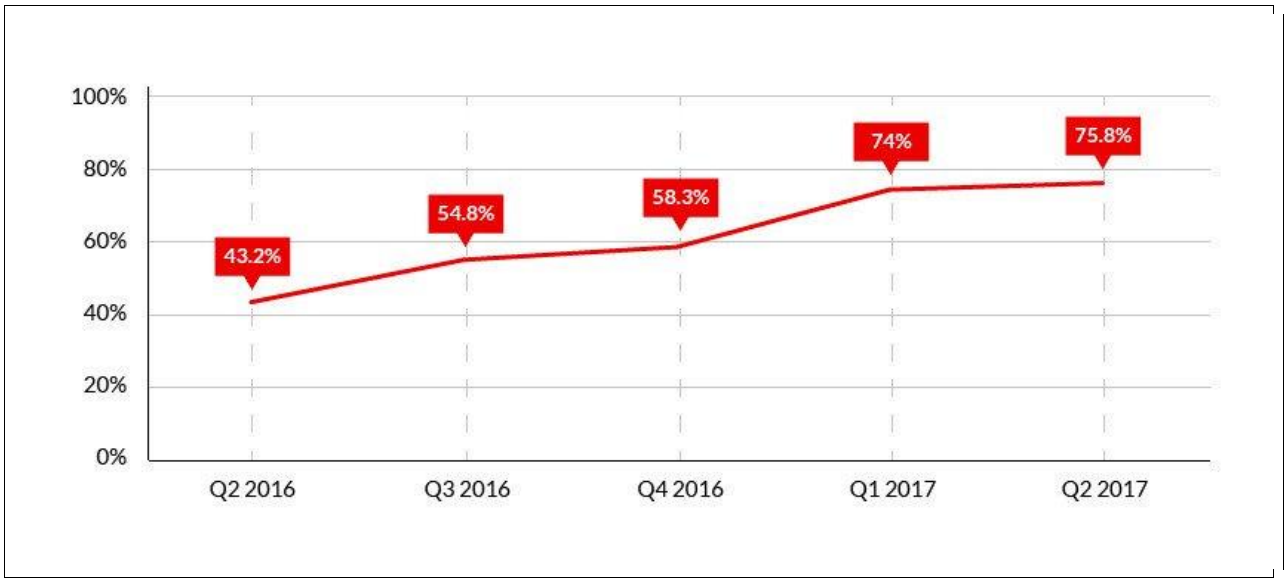
In any case, this study reveals an increase in the frequency of repetition of application-layer attacks. In total, 75.8% of web sites were affected by repeated attacks, the highest percentage ever has been reflected in a study of these characteristics. This method of attack has also been identified in the largest assault of the quarter, which reached a peak of more than 350 Gbps.

The complexity of the attacks is rising and this is reflected in the increased threats multivectoriales, which accounted for 40.5% of all DDoS attacks at the network layer, by 29% in the previous quarter.



The greatest attack from the network layer reached a maximum of 350 Gbps

The study of Imperva also reveals an upward trend in the number of persistent attacks at the application layer, which is increased for the fifth consecutive quarter.



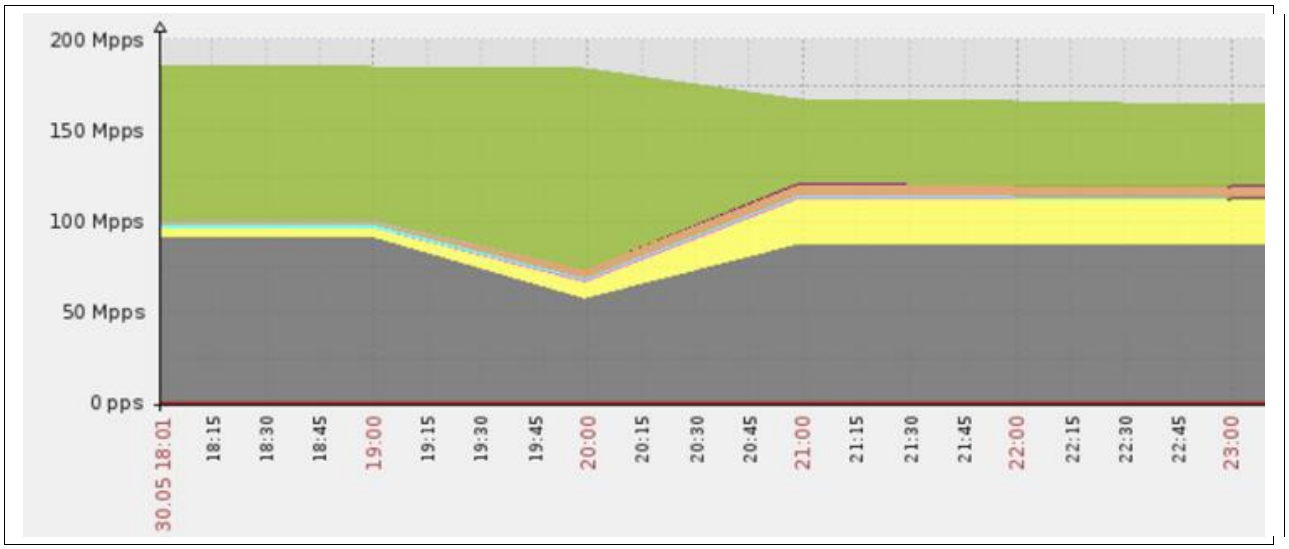
Number of objectives subject to repeated DDoS attacks

Attacks to the network layer

This study is based on the 2,618 attacks to the network layer (level 3 and 4) Mitigated by Imperva Incapsula in the second quarter of 2017, an average of 196 per week, compared to the 269 per week in the previous quarter. This represents a decrease of 35.9% compared with the first quarter of 2017 and was the fourth consecutive drop since the peak in the second quarter of 2016.

The trend toward short-term attacks continued, although at a slightly slower rate. 82.5% of the attacks to the network layer lasted less than 30 minutes this quarter, compared to 90.5% in the first quarter of 2017.

Although the main reason for these attacks continues to infect systems to increase the activity of bots, the appearance of these attacks distributed denial-of-service "wave" has been an important factor. The greatest attack of the quarter, which reached a peak of more than 350 Gbps, reached its peak in 190 Mpps.



The greatest attack in the second quarter of 2017 peaked at 190 Mpps

The attack time of the second quarter of last year lasted for more than 147 hours, a decrease of the assault of 204 hours that mitigate in the first quarter of 2017. However, the average duration of the attacks increased from 29 minutes to 34 minutes, with respect to the previous quarter.

After the record that was achieved in the first quarter, the use of multivectoriales attacks fell in the three months later, due in large part to the attacks of two vectors.

Length of attack

The second quarter of 2017 saw a continuation of the trend toward short burst attacks: the 91.7% lasted less than an hour. Although it is a very high rate, is slightly lower than the previous quarter.

The 82.5% of the attacks lasted less than half an hour and the majority of these attacks can be attributed to bots.

The number of attacks which lasted more than three hours in the second quarter of 2017 increased to 2.1 percent from 1.2 percent last quarter. On the contrary, only eight assaults lasted more than 12 hours this quarter, compared to 14 in the last quarter.

Vector attacks

As happened in the first quarter of 2017, the following were used several payloads ("payload") to run network-layer attacks, most of which consisted of a combination of attacks "flood" ICMP, TCP, UDP, and SYN.

The use of UDP and generic attacks "flood" TCP increased while the attacks "flood" ICMP and SYN decreased. While the tactics of attack to NTP and DNS have continued to use, only were present in 14.9% of the attacks.

Multivectoriales attacks

The multivectoriales attacks were reduced to 21.7% in the second quarter of 2017, after the historical record of the previous quarter: 40.5%. This can be attributed to the sharp decline in the attacks of two vectors, which fell from 33.5% to 9.4%. However, sophisticated cyber attacks continued to increase.

In the second quarter of 2017, the 12% of the attacks using more than three vectors, compared with 7% in the last quarter. Of these, the 2.3% used five or more vectors, compared with only 1.1%.

Attacks on the application layer

Imperva Incapsula mitigated 12,285 attacks on the application layer (level 7) during the second quarter of 2017, an average of 973 a week. With a reduction of 18% compared to the previous quarter, there were 1,099 attacks.

The greatest attack from the application layer in this quarter reached a maximum of 89,134 Rps (requests per second), which was

significantly lower than the attack of the last quarter with 176,393 RPS. The attack of this quarter, however, lasted 48 days, more than double that of the first quarter of 2017.

There was a significant increase in the number of goals that suffered repeated attacks at the application layer, another record in the records of Imperva Incapsula.

Duration of the attack and frequency

More than half of the attacks on the application layer lasted less than half an hour, dropping only one point in comparison with the first quarter of 2017 (58.8% to 57.4%).

Having said that, the amount of persistent attacks increase: the 7.4% lasted more than six hours, compared with 5.5% in the previous quarter. And of these, 1.7% lasted more than 24 hours.

In addition to the persistent increase in attacks, the frequency of attack reached a record. On average, only one objective was attacked 11.5 times during the quarter, while 19.5% of the objectives were achieved more than ten times.

Capabilities of the bots, and impersonation of systems

In the second quarter of 2017, the amount of bots advanced able to bypass security measures, i.e., retain cookies and/or execute JavaScript, fell to 2.1% from 9.6% in the first quarter of 2017.

Experience shows that this number tends to fluctuate according to the nature of the bots used for attacks according to that month. On the contrary, the number of bots primitive grew from 90.4% to 97.9%.
The bots DDoS attacks often try to evade detection through the use of fake user agents to masquerade as legitimate tools and browsers.

In the second quarter of 2017, the number of bots that enmascaraban as browsers, that is to say, Internet Explorer, Google Chrome and Firefox, increased from 85.6% to 92.1%.

The adoption of these default 'identities' is another sign of what little sophisticated attacks are the application layer that occurred this quarter.

Instead of trying to circumvent the security measures, the cybercriminals preferred to wage wars of attrition with persistent attacks of bots rudimentary.

Geolocation

The study by Imperva points to China as responsible for the 63% of the attacks, because they originated in its territory with 360.000 devices of attack. The US is in the second place, far from the eastern country (6.4%). But the most significant increases in proportion have been detected in India (5° with the 1.8%), Ukraine (4° with a 1.9%) or Turkey, where the activity of the bots has doubled, reaching 2.1%, occupying the third place.

In Turkey, we recorded more than 3,000 devices that generated more than 800 million applications from attack, more than double what we saw last quarter. In Ukraine and India, we recorded 4,300 devices, which represents an increase of approximately 75% from the first quarter of 2017. The combined attack of Ukraine and India was 1,450 million requests per quarter.

The US continues to be the country most affected by the cyber attacks due to the spate of attacks "pulse wave" against a relatively small number of sites, a trend that has continued since the first quarter of the year.

The 38% of the objectives in the US were exposed to six or more DDoS attacks in the course of the quarter, and the 23% were the target of ten or more attacks. In addition, out of the 45 objectives who suffered more than 50 attacks, 34 were sites hosted in the United States. The United States.

As a result of these repeated attacks, US. The United States was still the goal of more than 79.7% of all attacks, in spite of the house "only" the 61.4% of the objectives.

On the other hand, Spain (2.1%) shares the top 3 countries attacked with United Kingdom (2.1%) and the USA.

Link to the Imperva Report (in English):
https://www.incapsula.com/ddos-report/ddos-report-q2-2017.html

Aiuken Cybersecurity