Eleven Paths

Discovering Microsoft's Vulnerabilities: Who is Who

An Analysis on the vulnerabilities discovered in Microsoft products, their discoverers as well as their grade of severity

elevenpaths.com

Telefónica CYBER SECURITY UNIT

ÍNDEX

Over this report we will address the doubts as to how many flaws Microsoft detects in its own code, how severe they are, the trend they follow and how many flaws are found by third parties either through recognition programs or their own means.

Who finds more vulnerabilities in Microsoft products? **What percentage of vulnerabilities are discovered by Microsoft, other companies or vulnerability brokers? How many flaws have unknown discoverers?** Over this report we have analyzed the data of the last three and a half years with the aim of understanding who fixes what in the world of Microsoft products as well as the severity of these flaws. **Thanks to this report we will gain an interesting insight into who really investigates Microsoft products, reports them in a responsible manner, as well as how many vulnerabilities are attributed to someone and how many are not** (which might suggest that they are discovered by attackers).

On the second Tuesday of each month, Microsoft publish their traditional security patches in a single package to update Windows. Such update fixes a number of CVEs or vulnerabilities. However, this has not been always the case. For many years, they published bulletins hiding several CVEs, usually grouped by product.

For many years, Microsoft have incorporated in their Security Development Lifecycle practices an audit of their own code with the aim of improving their security. We wished to know exactly how many security flaws are found by the company over their internal audits **to get an idea not only of how much Microsoft contribute to the improvement of their products in terms of security, but also of how much the rest of usual 'bug hunters' of the industry do it.**

Executive Summary

- Google report over 17% of the vulnerabilities found in Microsoft products. Around 25% of the flaws are reported by the category 'other', that includes small companies that do not usually report, or freelance analysts.
- The third position is for Microsoft, since they detect more than 10% of their own flaws. They are followed very closely by the Chinese Qihoo 360, which nevertheless find more severe vulnerabilities than Microsoft.
- NCSC, iDefense and Check Point often report vulnerabilities with a severity over 5. In general, almost half of them are granted a severity degree of 8.
- In 2017 and 2018, Google led the number of vulnerabilities fixed in Microsoft products. Since 2016, the flaws found by Microsoft have been on the increase. However, during 2019 Qihoo 360 and ZDI have found a great number of vulnerabilities.
- Only 2% of attributes vulnerabilities are of maximum severity.
- In 2016, 25% of vulnerabilities were not attributed to anyone in particular. In 2019 (until September), only 9% of the vulnerabilities did not have a specific author. This may suggest that the number of flaws responsibly reported might have improved.

A Little Background

Microsoft have developed a lot their update policy. Since the chaotic emergence of patches in the late 1990s (with no control over which one preceded the other), including ridiculous moments when patches were published and distributed firstly in English and some days later in other languages. However, currently this process is completely automated and programmed so the whole system has been improved. But this has not been always the case. Since 2003 and for many years, it was possible to standardize in some way the Tuesday bulletins, until February 2017, when the well-known bulletins including the CVEs (from MS98-01 to MS17-023) stopped being published. This has been one of the most radical changes so far.

With the launch of Windows 10 in 2016, they broke away from what was already done. New nomenclatures appeared:

- **Security Only Quality Update**: It only contains security patches. They are released on the second Tuesday of each month.
- **Security Monthly Quality Rollup**: It includes the security and other features.
- **Preview of Monthly Quality Rollup**: This is optional, and is released one week after the second Tuesday of each month. It may be useful if you wish to know the impact of non-security related updates to be released the next month. That is, is a non-security related subgroup of what is going to be released the following month.
- Since 2016 the monthly number of vulnerabilities has been progressively reduced, such vulnerabilities being reported but non attributed. On average, from 25% in 2016 to 8% in 2019.

Over this report we will analyze what vendors contribute more to fix the CVEs distributed into these packages.

Methodology

We have performed a very simple analysis. **We have collected and processed all the information of attributed CVEs from March 2016 to September 2019.** The source of information has been mainly the following webpage:

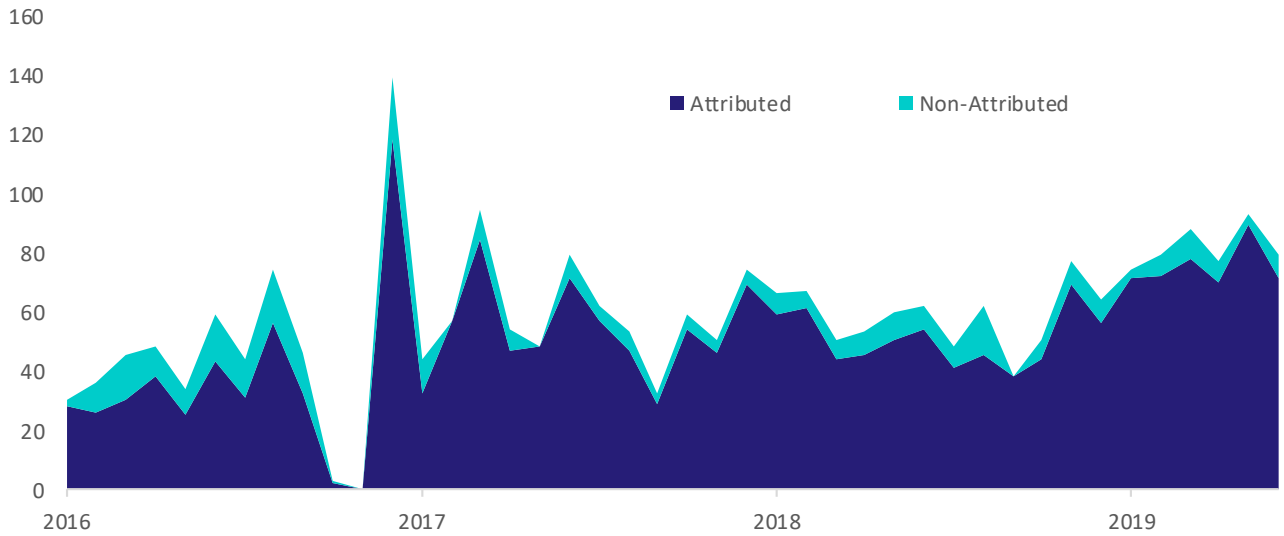
https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments

These are the attributed vulnerabilities (that is, the ones reported by a given identifiable user, either individual or company). In 2019 (until September), we have analyzed 621 attributed vulnerabilities. 607 in 2018, 593 in 2017 and 310 in 2016 (only since April). **This represents a total of 2,131 vulnerabilities analyzed.** From all of them, we have extracted their severity through the NIST's official CVSS.

Nevertheless, these figures do not represent the total number of flaws discovered every month or year. Actually, we have also considered those flaws that were not directly attributed. **We understand that most of these flaws may come from vulnerabilities found in 0-days or under other circumstances where the author is not known (and the vulnerability has not been reported anonymously).** In such cases, Microsoft do not attribute the finding to anyone in particular. This difference between attributed and 'non- attributed' vulnerabilities (which is not the same as 'anonymous') is represented in the following chart.

NOT ALL VULNERABILITIES ARE ATTRIBUTED

Number of vulnerabilities attributed and non-attributed from 2016 to 2019



From the credits, we have extracted the company that found the vulnerability. **If there were several discoverers, we have considered only the one that appeared in the first place in order to make the calculations simpler** and since we understand that the one who reported them first is shown as the main analyst. While this might be inaccurate, it results in the simplest formula. Moreover, we have considered two flaws found by the Hiper-V team as discovered by Microsoft.

From that point, we have performed different calculations to analyze who contributes more and better to improve the security of Microsoft products, in a responsible manner.

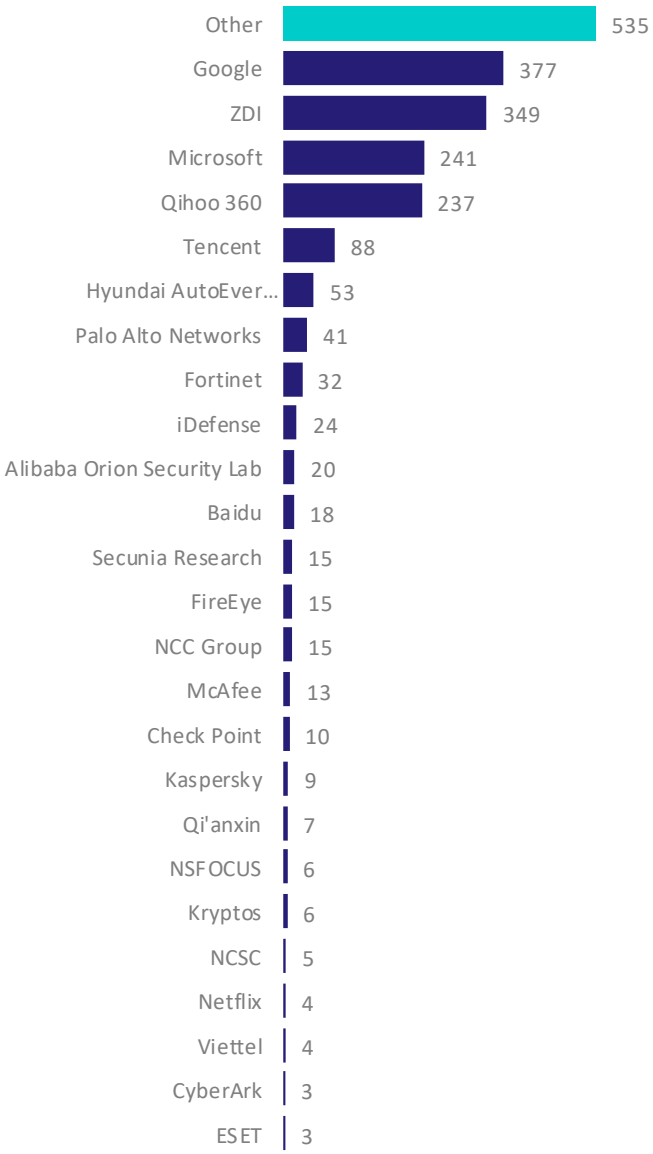
The Data

Google (normally through their Zero Day Project) is undoubtedly the company that most collaborates in the reporting of vulnerabilities in Microsoft products: they report over 17% of the flaws. Around 25% of the flaws found in Microsoft products are reported by the category 'other', which includes small companies that do not usually report, or freelance analysts. The third position is for Microsoft, since they detect more than 10% of their own flaws. The Chinese company Qihoo 360 find almost the same number of flaws.

Trend Micro's Zero Day Initiative is a private initiative that acts as a vulnerability 'broker'. Researchers may subscribe to this program and will be rewarded for every vulnerability found in exchange of giving them up to ZDI, that will report them to the vendors in a responsible manner. This initiative is the most popular formula: nearly as many vulnerabilities as Google are reported to Microsoft.

GOOGLE IS THE COMPANY FINDING MORE VULNERABILITIES IN MICROSOFT'S PRODUCTS

Total Number of Vulneabilities by Discoverer from April 2016 to Sept 2019

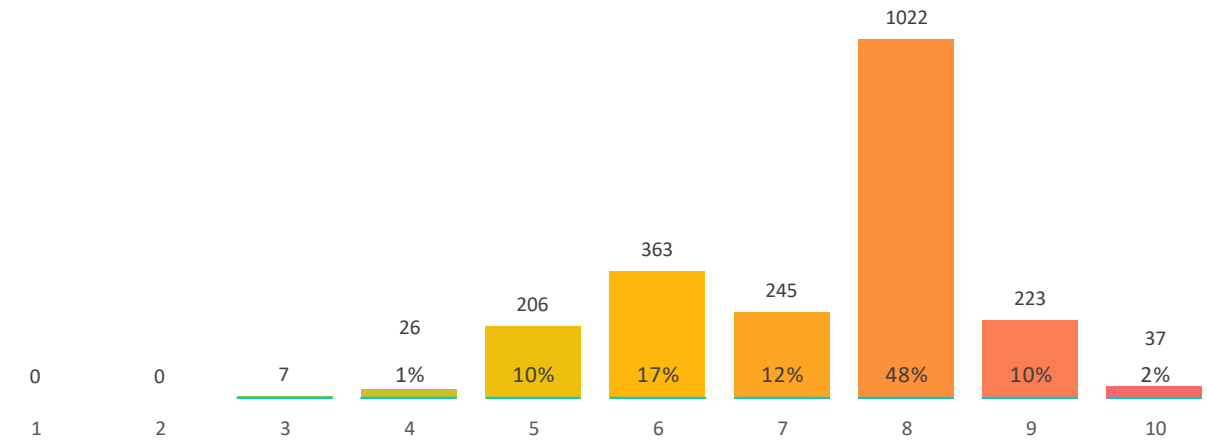


Most vulnerabilities in Microsoft's products have a score around 8

The following graph represents the analysis of the severity of these attributed vulnerabilities, from 1 to 10. Almost half of the vulnerabilities are given a severity of 8. Very few of them, barely 2%, are of maximum severity.

MOST VULNERABILITIES IN MICROSOFT'S PRODUCTS HAVE A SCORE AROUND 8

Vulnerability distribution by CVSS Score, from April 2016 to Sept 2019

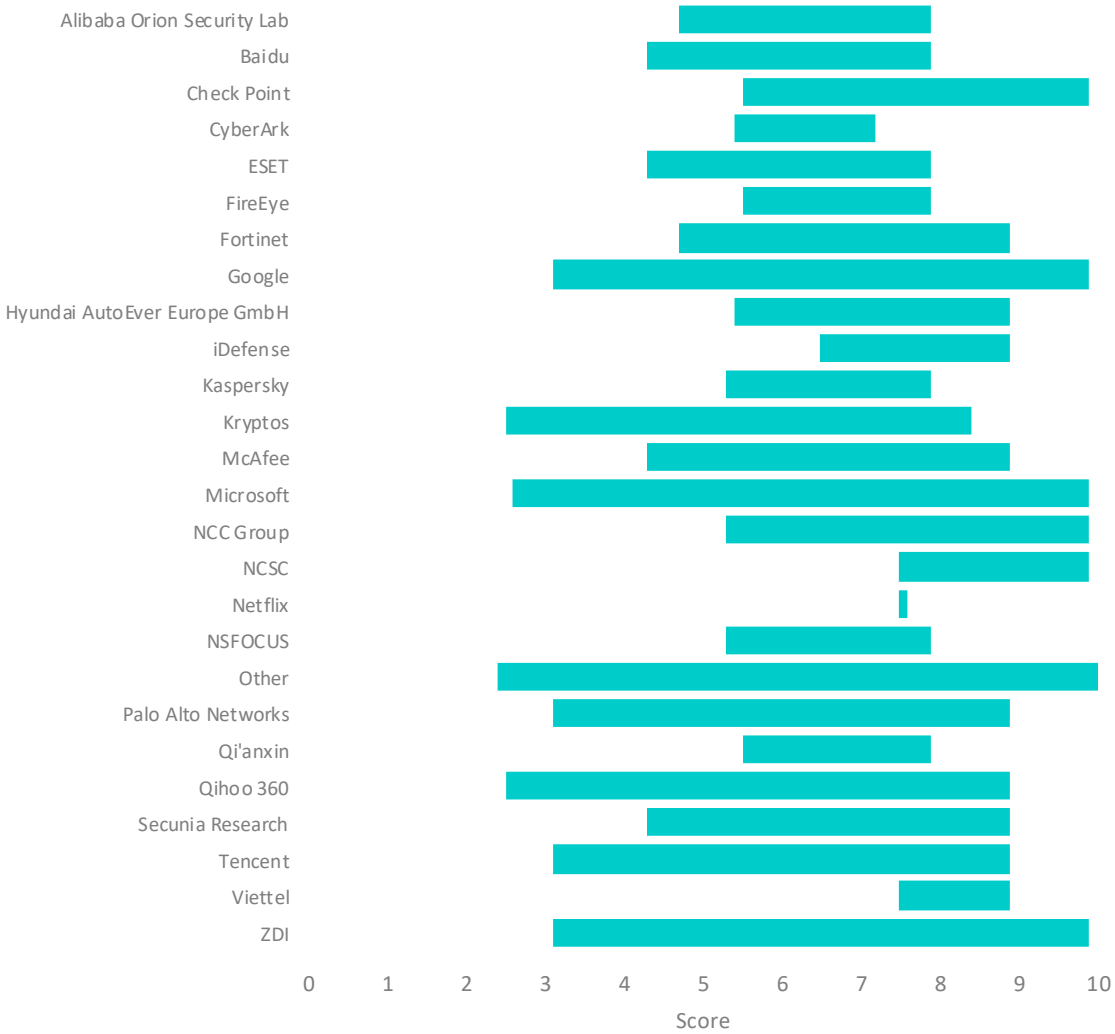


The more vulnerabilities reported by a company, the wider the range of severity

This chart analyzes the **potential 'specializations'** of those who find vulnerabilities, the range of severity **they cover**. The field 'other' and ZDI (which includes other researchers who prefer to report through this broker) monopolize the greater range of vulnerability severity. The chart shows that NCSC, iDefense and Check Point usually report vulnerabilities with a severity above 5.

THE MORE VULNERABILITIES REPORTED BY A SOURCE, THE WIDER THE RANGE OF SEVERITY

Range of Score, by Source

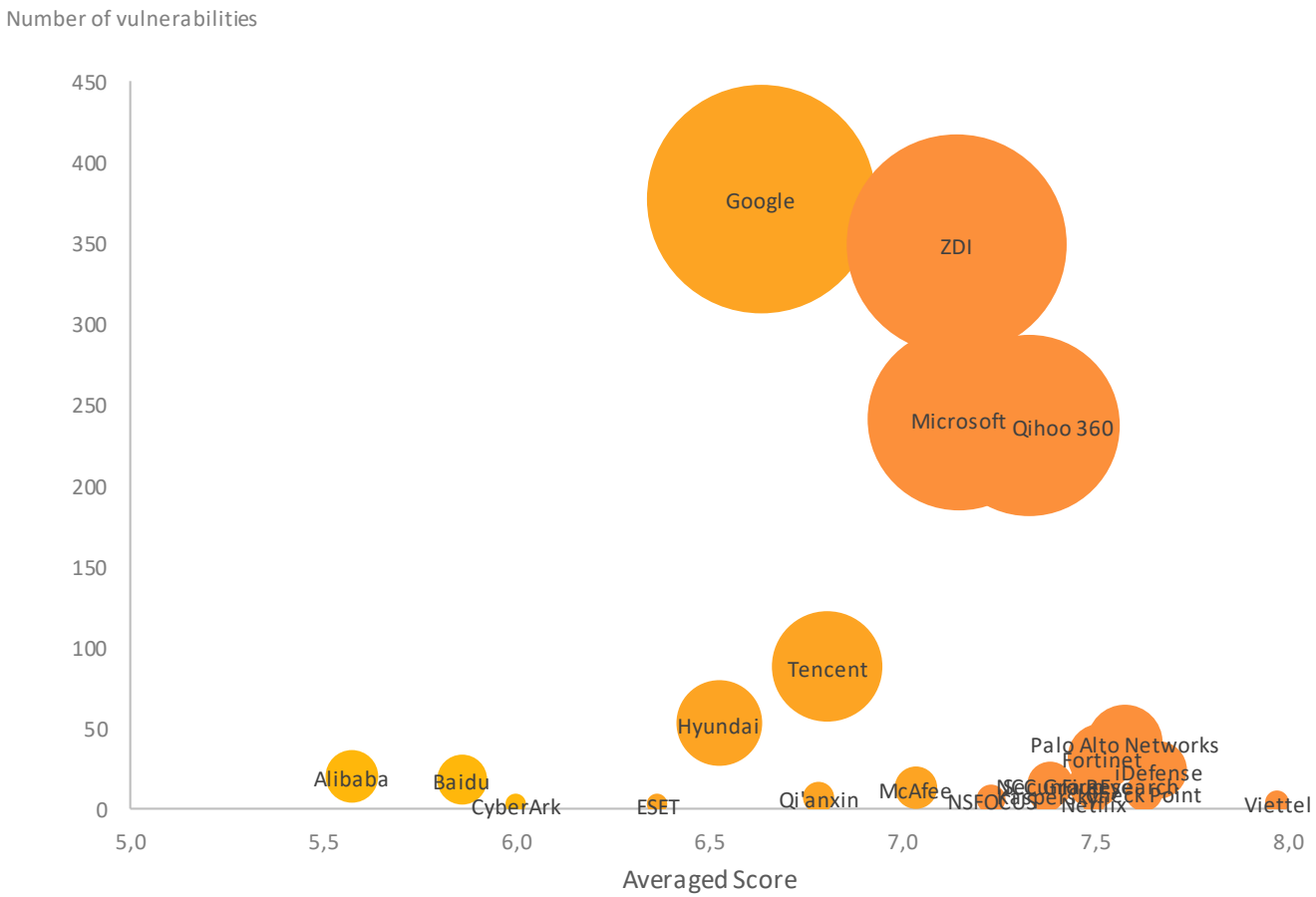


Google reports more vulnerabilities, but of lesser severity

If we correlate both values (severity and number), we observe that **although Google find indisputably more than any other vendor, they move within a range of gravity lesser than that of Microsoft.** Those reported by Qihoo, which find almost the same number of flaws as Microsoft, are usually of a greater severity.

GOOGLE REPORTS MORE VULNERABILITIES, BUT OF LESSER SEVERITY

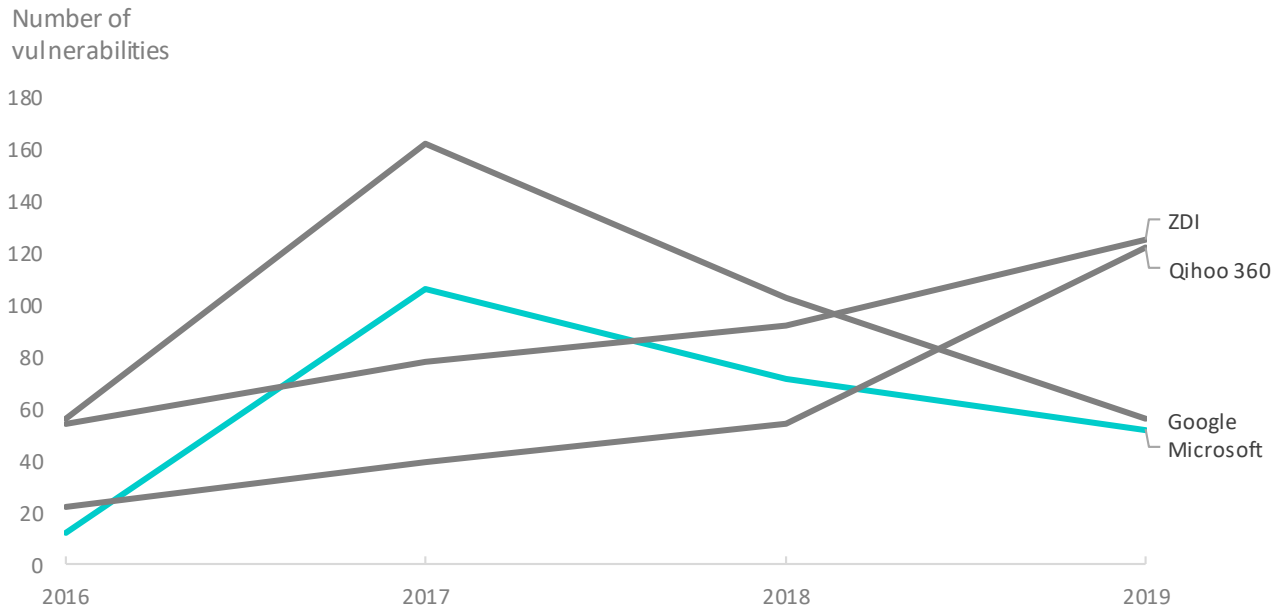
Vulnerability distribution by Score and Discoverer; bubble size is proportional to the number of vulnerabilities found



ZDI and Qihoo 360 are discovering more vulnerabilities every year

The following chart shows the evolution of these researchers throughout the years. We can see that in 2017 and 2018 Google led the number of vulnerabilities fixed in Microsoft products. Without a doubt, **since 2016 Microsoft have found more and more flaws**, but Qihoo 360 and the ZDI broker (which includes freelance researchers) have had a 2019 full of vulnerabilities.

ZDI AND QIHOO 360 ARE DISCOVERING MORE AND MORE VULNERABILITIES EVERY YEAR
Vulnerabilities found by the four major contributors



The ZDI initiative seems to have become itself the most important way to report vulnerabilities in 2019, since it encompasses all kind of independent researches —while Microsoft and Google have lost relevance during this year.

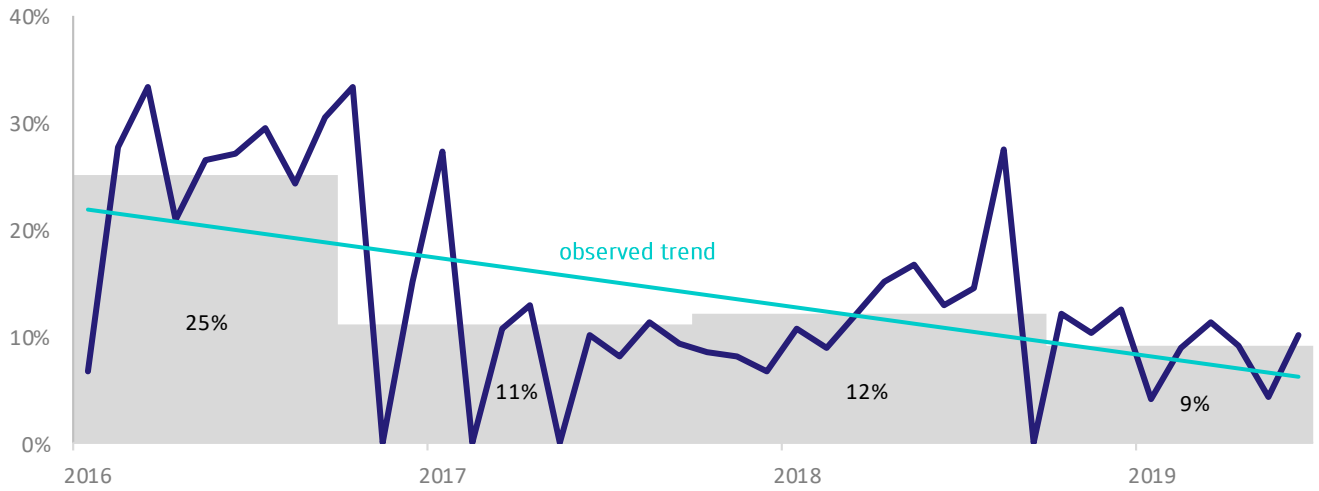
Non-attributed Vulnerabilities

With respect to non-attributed vulnerabilities, the data is very interesting. We have calculated, per month and year, **what percentage of vulnerabilities did not appear as attributed, and we may conclude that most of them were found by attackers or have not been reported through the usual responsible disclosure channels.** It must be noted that this does not include anonymous reports, which can be communicated in a fully responsible manner while remaining anonymous –in this kind of vulnerabilities the discoverer is not directly known, and in most cases it may be an attacker.

In 2016, 25% of the vulnerabilities were not attributed to anyone in particular. In 2017, the percentage dropped to just over 9%. In 2018 it rose slightly to 11%. Finally, in 2019 (until September), only 9% of the vulnerabilities did not have a specific author. **This may suggest that the number of flaws responsibly reported might have improved.**

VULNERABILITIES ARE BEING DISCOVERED AND REPORTED MORE RESPONSIBLY THROUGHOUT THE YEARS

Percentage of non-attributed vulnerabilities, possibly discovered by attackers; grey columns represent yearly total



Conclusions

Since 2016, Google has reported over 17% of the vulnerabilities found in Microsoft products. During 2019, ZDI and Qihoo have substantially raised the number of reported vulnerabilities. Around 25% of the flaws are reported by the category 'other', that includes small companies that do not usually report, or freelance analysts.

The third position is for Microsoft, since they detect more than 10% of their own flaws. However, the number of vulnerabilities found have decreased during the last two years. In 2016, 25% of vulnerabilities were not attributed to anyone in particular. In 2019 (until September), only 9% of the vulnerabilities did not have a specific author. This may suggest that the number of flaws responsibly reported might have improved. Only 2% of the attributed vulnerabilities are of maximum severity.

We may conclude that most of the vulnerabilities found in Microsoft (most of them with a severity of 8) are discovered by four main actors: Google, Qihoo, ZDI (that include independent researchers) and Microsoft. Over the last years the roles have changed, since Google and Microsoft have handed the first positions over to ZDI and Qihoo. It must be also noted the significant drop of non-attributed vulnerabilities (which are found in a non-responsible manner). From 25% in 2016 to 9% in 2019, which suggests a better vulnerability management, indeed via platforms as ZDI, where researchers are rewarded and encouraged to report vulnerabilities in a responsible way.

About ElevenPaths

At ElevenPaths, the Telefónica's Cybersecurity Unit, we believe in the idea of challenging the current state of security, since security constitutes a feature that must be always present in technology. We are continuously redefining the relationship between security and people, with the aim of developing innovative products capable of renovating the concept of security. Thanks to this, we stay a step ahead of attackers, that are increasingly present in our digital life.