KASPERSKY lab

Kaspersky Security Network Report: Windows usage & vulnerabilities

Version 1.0, August, 2014

Contents

Introduction: the place of the PC in our multi-device world

These days few people are content to settle for a single personal communications device. The comfort, functionality and relative affordability of smartphones and tablets are attracting millions of users all over the world. Previously people used only a PC or a laptop for communication on the Internet, online shopping, games or other activities; now they are using smartphones, tablet and other 'connected' devices for many of these purposes. These devices are also becoming more diverse - various portable devices, TVs , cars, etc.

In this situation, the role of personal computers in the life of modern people has changed significantly: it is now only one of the devices used in their daily lives. This change has affected the global PC market - in 2013 it experienced a 10% drop which according to the analytical company Gartner represents its biggest decline on record. In 2014, the decline of the PC and laptop market continued: according to Gartner, in the first quarter of 2014, PC production decreased by 1.7% compared to the same period in 2013.

The shift in consumer preferences away from standard PCs and laptops is obvious, but rumors of the imminent death of the PC are hugely exaggerated. Just because PC users are buying smartphones and tablets instead of upgrading their PCs, it doesn't mean they are hurrying to throw away their old computers. PCs are still a familiar fixture in living rooms and children's rooms, where they still fulfill a role as a stationary terminal to access the Internet, play games, watch video footage and explore other multimedia content.

It's a similar story when it comes to the IT security: although the number of devices running under mobile operating systems - iOS, Android, Windows Phone - is constantly growing, the vast majority of existing cyber threats are still primarily aimed at PC users and Windows OS. Windows, which is the most common operating system on these devices, is a well-developed global software ecosystem which used to be the test bed for the whole hacker underground as it evolved into an independent parallel ecosystem with a black market of illegal software and services.

The symbiotic relationship between cybercrime and Windows is so strong that it will only be broken by the appearance of other competitive and widespread software platforms, or by the collapse in the sales of PCs and laptops. The statistics that Kaspersky Lab receives from Kaspersky Security Network reinforce this trend. Over 60 million KSN subscribers worldwide voluntarily share data about the threats which they have encountered while working on their computers. This information helps Kaspersky Lab to respond quickly to new threats and almost instantly deliver the information necessary to combat these threats to the users. According to our statistics, the number of these threats is extremely high: in 2013, Kaspersky Lab products blocked attacks over 5 billion attacks. Every day the company experts and automatic detection systems detected about 315,000 malicious programs. In 2012, this figure was around 200,000.

And, of course, the overwhelming majority of threats detected daily were created to attack the users of Windows OS.

Why Windows?

When we choose a topic for the next report based on statistics collected from Kaspersky Security Network, we try to pay attention to the most interesting threats or software platforms. For example, the years 2012-2013 were dominated by the rapid growth in the number of vulnerabilities in the Java environment and exploits for them, so we decided to prepare a special investigation of attacks on this platform. In 2013, Kaspersky Lab analysts saw an increase in the number of cyber-attacks targeting financial information, which inspired a more detailed investigation of such attacks.

For Windows OS, the last six months have been really interesting. Last October, Microsoft released its latest version, Windows 8.1, which was also the first version to form part of the new annual release strategy. In April, the company almost completely[1] stopped supporting Windows XP, one of the most popular operating systems on the market since 2001 (for more than 13 years).

The combination of an OS which is no longer supported by the developer, and a dangerous vulnerability in one of its components or a related piece of software is a nightmare scenario for information security. That is why Kaspersky Lab experts decided to focus on three key metrics in this research: the distribution of the Windows version which is exploited by the users of Kaspersky Lab products, the dynamics of migration to the latest version of this software, and the landscape of attacks using exploits written for the vulnerabilities in Windows and other widely-installed Microsoft software.

Methodology and accuracy of the report

This investigation studied the level of exploits targeting the versions of Windows OS belonging to the users[2] of Kaspersky Lab products who agreed to provide data to Kaspersky Security Network. The main systems under review were Windows 8.1, Windows 8, Windows 7, Windows Vista and Windows XP, and their variants. These systems are used by the overwhelming majority of the users of Kaspersky Lab products. A further object of the research was information about detected exploits which used vulnerabilities in Windows and other Microsoft products.

These parameters were examined in terms of the geographical distribution and changes over time.

The study period was the 8 months from November 2013 to June 2014. However in some cases the results were compared on a month-to-month basis (for example, the results for June 2014 were compared with the results for June 2013).

[1] Except XP Embedded
[2] The study considered KSN participants who faced at least one malware incident over the reporting period

The ultimate goal of this study was to find out how quickly users migrated to newer versions of the system and how much risk of users faced if they did not update promptly and faced exploit-based attacks utilizing vulnerabilities in out-of-date Microsoft products.

During the research we analyzed the information received from over 60 million users worldwide. Is this selection big enough to draw any meaningful conclusions regarding the behavior of Windows users?

To find out, we turned to a third-party source – the famous analytical service StatCounter.com and compared the data on the popularity of the operating systems from KSN and StatCounter. According to KSN, in June 2014 the picture was as follows:

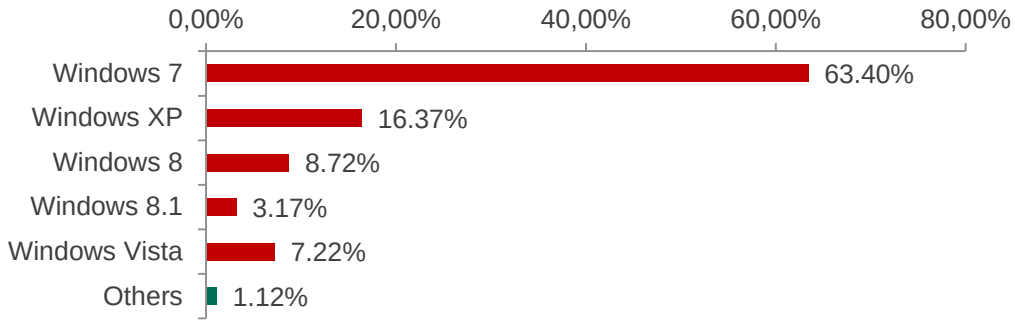

Fig.1: The most popular versions of Windows in use in June 2014 according to KSN (the number of unique users)

The data from StatCounter for the same period was as follows:

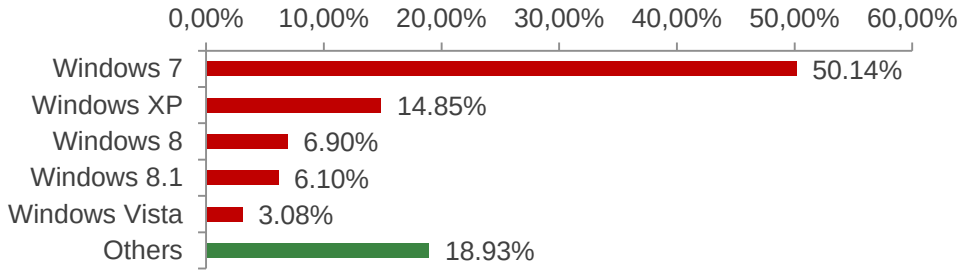

Fig.2: The most popular versions of Windows in use in June 2014 according to StatCounter

Of course, the figures in these two sources differ. First of all, because of the differences in how the data is collected: StatCounter keeps count of page views while Kaspersky Lab considers the number of unique users. However, the overall match between KSN and StatCounter's versions is obvious.

Main Findings

- Despite the fact that Microsoft completely stopped supporting Windows XP, many people are still using this system: in June, 16.37% of Kaspersky Lab customers worked on computers running Windows XP
- More than 18 months after its official release, 8.72% are using Windows 8. 7.22% are using Windows 8.1
- The newest Windows 8.1 system is most widespread in the USA, Canada, Germany and the UK
- The older Windows XP system is most widespread in Vietnam, China, India, Algeria and Spain
- Although vulnerabilities are regularly detected in Windows and other Microsoft products, the absolute majority of detections fall on exploits for just five vulnerabilities, the oldest of which was found in 2010.
- Four years after its detection the LNK vulnerability CVE-2010-2568 used to distribute the notorious Stuxnet worm is still a significant threat. Most detections of exploits for this vulnerability are registered in Vietnam, India, Indonesia, and Brazil.

More details about can be found in the study below.

Part 1. User migration dynamics: "Slow" Windows 8.1, "immortal" XP

Windows 8.1 OS, the current version of Microsoft's operating system, was released in mid-October 2013. This was an important event since Windows 8.1 is the first upgrade of Microsoft's planned new annual release schedule. In addition, this is the first system where migration from the previous version is performed via Windows Store: the access client to it is included in Windows 8.

The simplicity of this scheme should have affected the speed of migration to the most current system. Additionally, the speed of migration to the new OS should have been further accelerated by the end of support of Windows XP in April 2014. However, KSN's statistics paint a rather different picture.

Manifold Windows: the dynamics of measuring the popularity of different OS versions

The general dynamics of changes in the level of popularity for various Windows versions during the period under study looks like this:

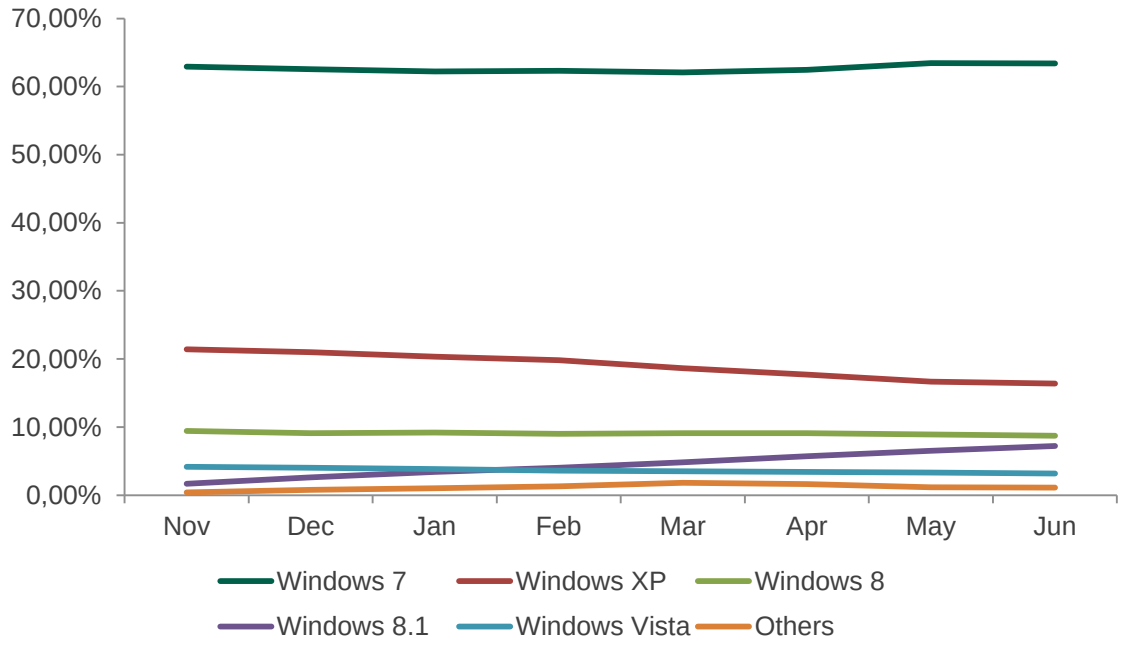

Fig. 3: The popularity of various Windows versions during the period under study from November 2013 to June 2014

As seen from the graph, Windows 7 is the clear leader and its share is growing: in November last year it was on 62.91% of machines, while in June 2014 it reached 63.4%. However, in

terms of absolute numbers, the growth from November to June is insignificant - just a few thousands of users – which does not add up to any important change. On the contrary, the number of Windows 7 users remains high despite the fact that the market offers more up-to-date systems. Noticeably, Windows 7 dominance is steady: for example, in June 2013 this system was user by 63.22% of people, almost the same as a year later.

With the popularity of the other Windows versions the situation was different. For clarity, we excluded Windows 7 figures from the chart below.

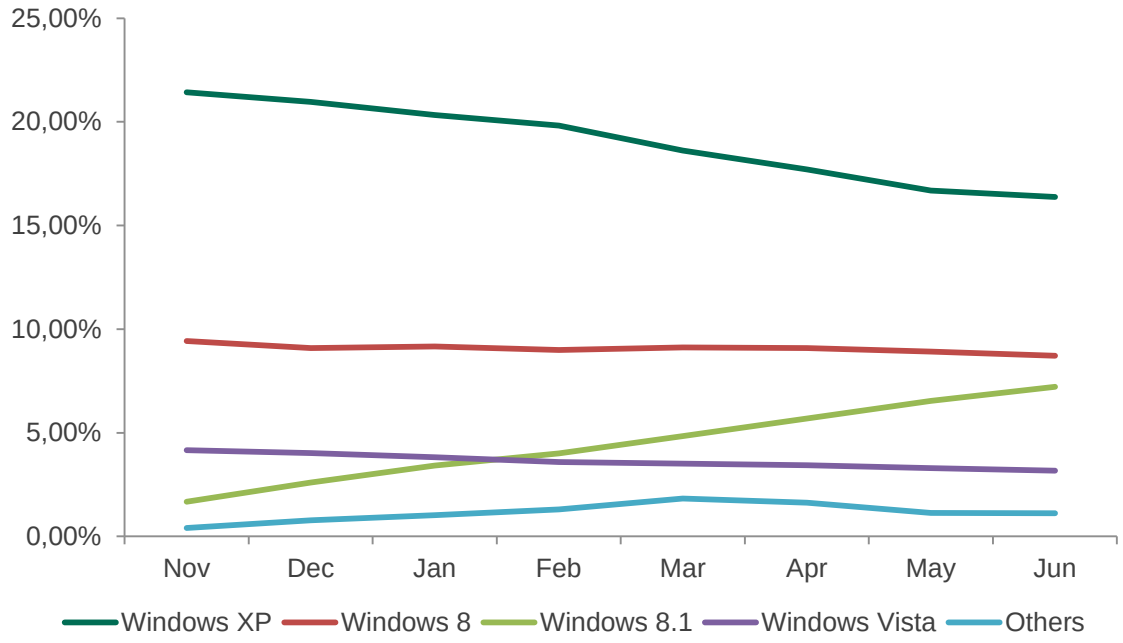

Fig. 4: The popularity of various Windows versions during the period under study from November 2013 to June 2014 (Windows 7 excluded)

As can be seen from the graph, the share of the 'ancient' Windows XP has finally started to drop considerably: from 21.42% in November 2013 to 16.37% in June 2014. The percentage of Windows Vista has declined less drastically - 4.16% at the beginning of the period to 3.17% at the end. Despite the availability of the more up-to-date version of the OS, Windows 8 still has 8-9%. As a newcomer, Windows 8.1 is gradually increasing its share from 1.67% in November to 7.22% in June.

This general picture shows the popularity of different Windows versions over the past eight months. Currently there are five versions that account for the majority of all users of Windows-based Kaspersky Lab products. However, there are only two that demand closer inspection right now: the very old but almost legendary Windows XP and the new arrival, Windows 8.1. The dynamics of these systems usage will be the focus of the following chapters of this report.

Windows 8.1 migration dynamics: slow in general but faster than Windows 8

As mentioned above, by the end of June 2014, more than six months after the release of Windows 8.1, the distribution of Microsoft OS versions by popularity is as follows:

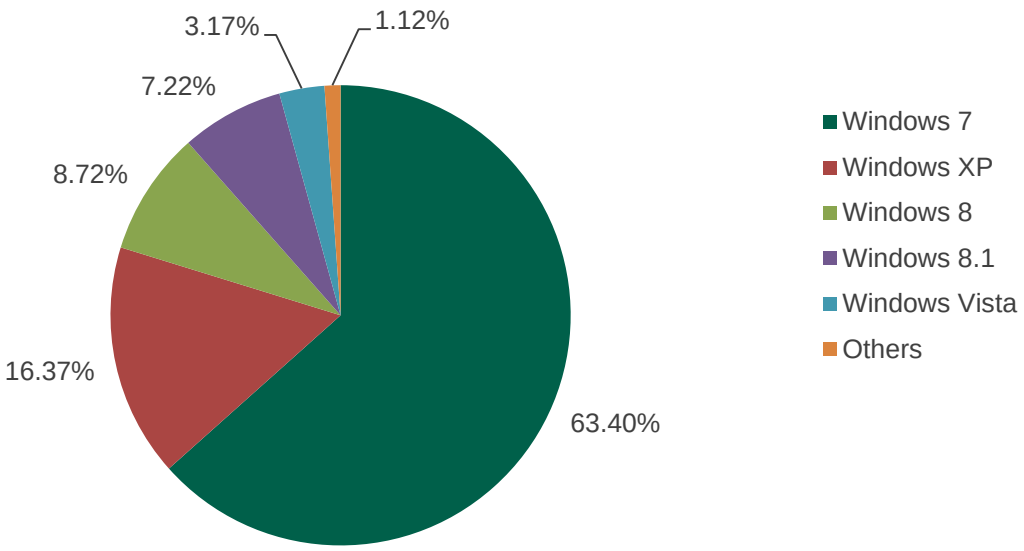

Fig 5.: Windows usage, June 2014 *Hereinafter the data is taken from Kaspersky Security Network*

Windows 8.1 accounted for only 7.22% of users, Windows 8 – 8.72% while the vast majority of users (63.4%) still prefer Windows 7. More than six months earlier, a month and a half after the release of Windows 8.1, the picture looked like this:

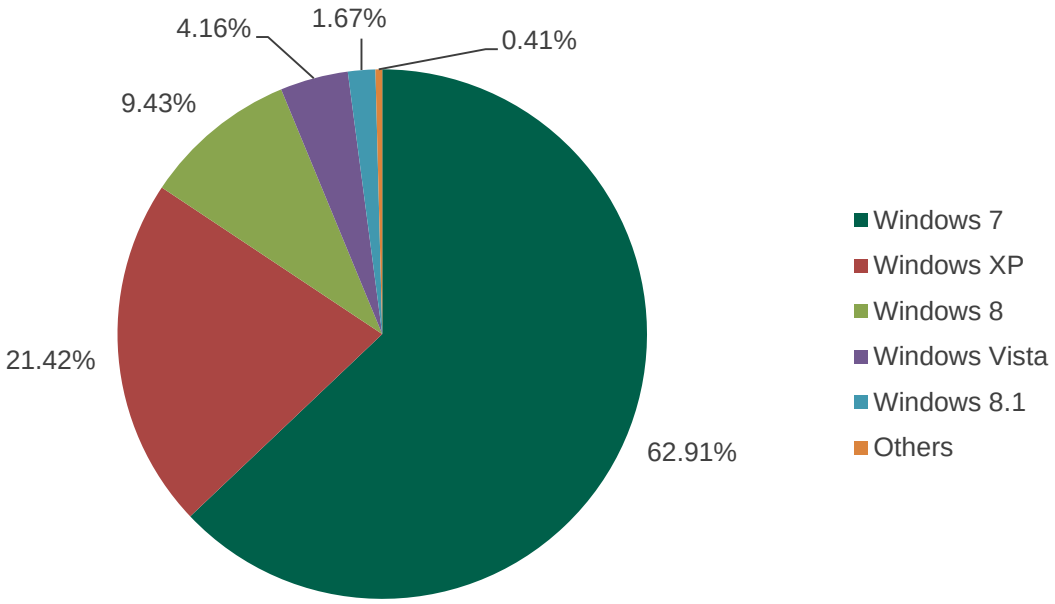

Fig.6: Windows usage, November 2013

In its first six weeks on release, Windows 8.1 attracted 1.67% of users. Over the subsequent seven months it added 5.55 percentage points. In order to understand whether those numbers are impressive or not, we need to turn to the earlier data and see how the number of Windows 8 users grew during the equivalent period of the previous year.

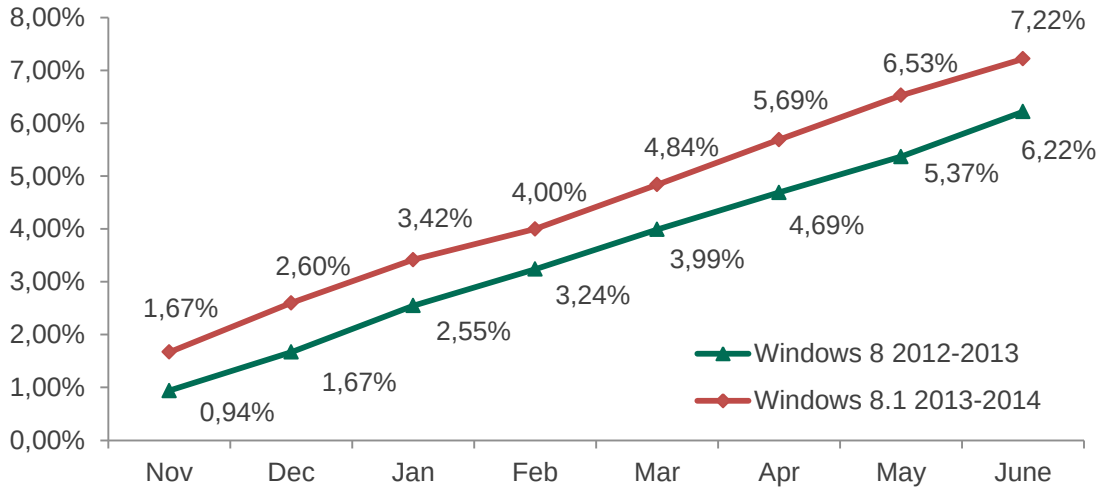

Fig. 7: The rate of increase in the proportion of Windows 8 users vs. Windows 8.1 users

As the graph shows, Windows 8.1 outperformed its predecessor: every month the system attracted somewhere between 0.7 and 1 percentage point more than Windows 8 had achieved the previous year. In absolute terms, after five months Windows 8.1 could match the number of users Windows 8 had after seven months. If we compare the total number of Windows 8.1 users, we can see that they are fast catching the total number with Windows 8. The two systems should claim an equal number of users sometime in September or October 2014.

Windows 8.1: the geographical spread

To understand where the percentage of Windows 8.1 users is the biggest, Kaspersky Lab identified the country with the highest absolute number of users of the system and analyzed what proportion of Windows users were using the most up-to-date product version.

According to this method, the list of countries with the most users of Kaspersky Lab products running under Windows 8.1 as of June 2014 is as follows

United States
Russian Federation
Germany
France
Brazil
United Kingdom
India
Mexico
Canada
Italy

However, when we look at the penetration rates for Windows 8.1 among all Windows users, we get a completely different chart.

United States	**16.2%**
Canada	**13.5%**
Germany	**11.1%**
United Kingdom	**10.8%**
France	**10.3%**
Mexico	**9.6%**
Brazil	**8.4%**
Italy	**8.1%**

Russian Federation	**5.14%**
India	**2.91%**

The USA, Canada, Germany, the UK and France are the countries where Windows 8.1 is most widespread, and are the only places where more than 10% of users have the latest system. Italy with 8.1% is some way behind its European neighbors. Mexico and Brazil are in the middle of the list. Russia (5.14%) and India which scored less than 3% are outsiders.

It's worth noting that the results for the previous version of Windows 8 are fairly similar to those for Windows 8.1: in June it was found on 12.48% of computers in the USA and 10.93% in Canada. The total share of Windows 8.x systems in these countries in June amounted to 28.75% and 24.45% respectively, i.e. in both cases this averaged around quarter of the total number of Windows users "visible" to Kaspersky Lab on specific markets. In June, the total share of Windows 8 and Windows 8.1 in Germany accounted for 17.24%; in the UK it was 17.91%. This is not a bad result for systems that appeared on the market only 18 months ago and that face competition from the well-established Windows 7.

This is a "portrait" of the latest Microsoft operating system made a little more than six months after its release. Next we will analyze the situation with the popularity of Windows XP – an OS with an especially interesting story over the past six months.

Windows XP – the OS that runs and runs

Windows XP was launched as a commercial product over 12 years ago, in 2001. It was taken off the market (as a retail product and a reinstallation on new computers) in 2010. Standard technical support for consumer versions of this system were also suspended at that time, and in April 2014 Microsoft ceased to provide enhanced support. According to Microsoft, Windows XP proved to be the most long-lived system in company history.

That claim is reinforced by Kaspersky Lab's data. In June 2013, 25.42% of users were running this system. In other words, barely one year ago, more than one in four owners of a Windows-based computer was using XP. In June 2012, it was used by more than one third (35.64%), while one year further back in 2011 it had almost half the market (47.86%). This year, in June 2014, XP was still faithfully serving 16.37% of users.

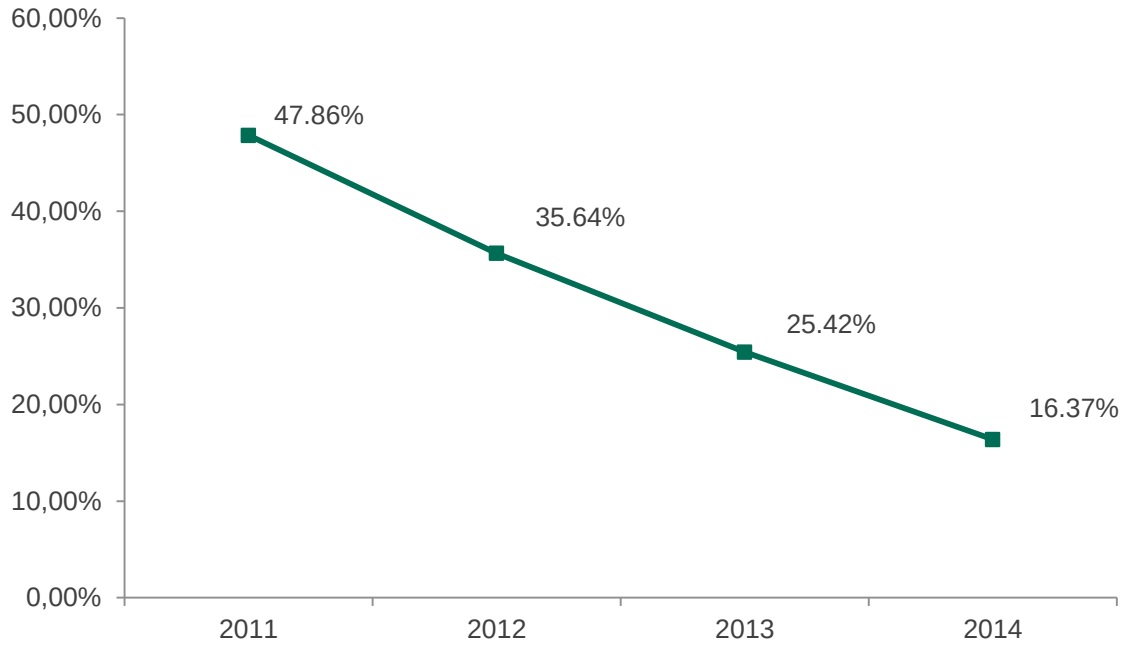

Fig. 8: Windows XP usage 2011-2014

While it's clear that XP's market share has been dropping steadily by around 10 percentage points a year, that rate of reduction has constantly slowed. From June 2011-2012, 12.22 p.p. of users abandoned the system. In the subsequent month 10.22 p.p. gave up XP and the decline in the year to June 2014 dropped to 9,05 p.p.

Even though by June 2014 standard support and the sales of the system had been unavailable for more than three years, XP still retains a high percentage of users. At the same time, as seen in the graph below, the external events that should have hastened the system's demise – the release of Windows 8.1 in October or the end of XP support in April – did not have any real impact on the numbers.

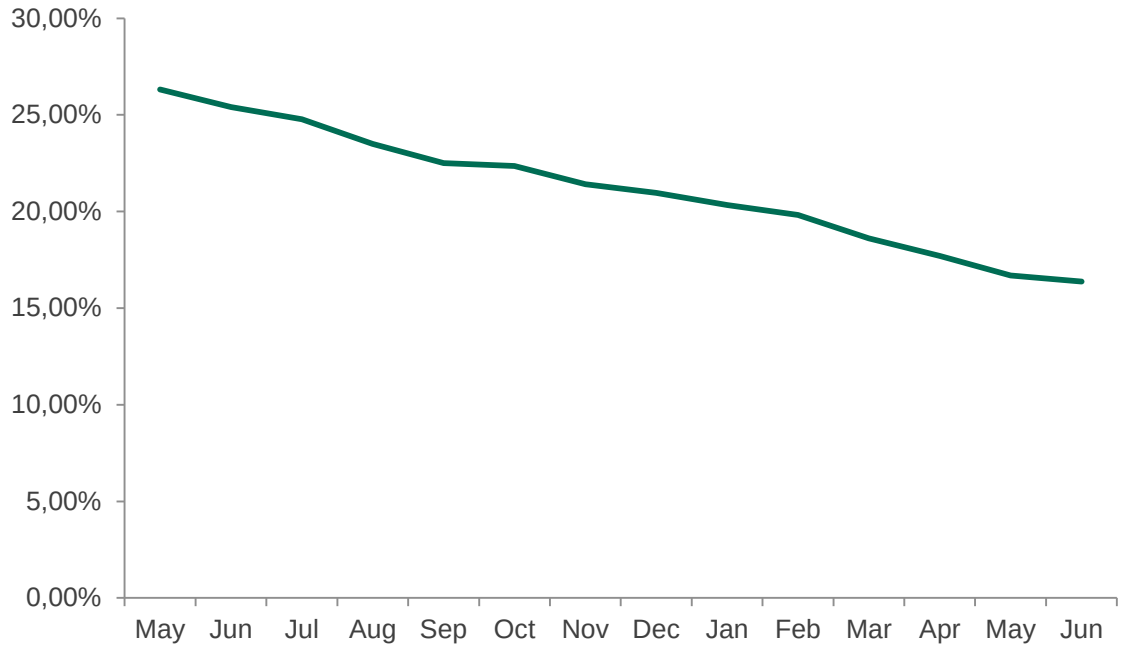

Fig.9: XP's failing market share 2013-14

At its current rate the proportion of the system users will drop to 5-7% by June 2015 and it will take about six more months for XP to drop out of the list of the most popular systems

The reasons for XP's longevity are clear: after a series of not entirely successful Windows launches - 98, 2000, and Windows ME - XP was a real breakthrough with its high speed and relative stability. Windows Vista released in November 2006 was regarded by many users seen as a step back: this system faced a storm of criticism while the reliable and efficient XP was something of a safe haven that even lured users back from Vista.

As a result, when Microsoft launched Windows 7 in 2009, and helped to rebuild its reputation as a developer of high-quality and fast software products, the completely outdated XP was now the improbably benchmark for a "high-quality operating system"

It is highly likely that this positive reputation explains XP users' reluctance to abandon the system. Yet another factor is the unofficial versions and builds. Since the introduction of the system enthusiasts have had plenty of time to develop their own XP-related modifications. Kaspersky Security Network includes more than 160 modifications, of which only about a dozen are official versions released by Microsoft. Of course, most of these modifications and distributed free of charge and this is yet another strong factor in XP's enviable vitality.

Although the time and competition from more up-to-date systems is pushing XP out of the market, there are still many countries in the world where this system will maintain a significant market share for many years to come.

Windows XP: the geographical spread

North America and Europe are the leaders for the latest operating systems, such as Windows 8 and Windows 8.1, but the picture for Windows XP is very different.

As with Windows 8.1, in order to identify the leader we first selected the countries with the highest absolute number of Windows XP users and determined the percentage of computers running XP. The Top 10 countries for absolute numbers of XP users looks like this:

Russian Federation
Vietnam
India
Germany
Italy
United States
Algeria
China
France
Spain

In June these 10 countries had more than 65% of all XP users. The percentage of XP users in these countries is as follows:

Vietnam	**38.8%**
China	**27.3%**
India	**26.9%**
Algeria	**24.2%**
Italy	**20.3%**
Spain	**19.2%**
Russian Federation	**17.4%**
France	**12.04%**
Germany	**8.5%**
United States	**4.5%**

As can be seen from the table, Vietnam is the absolute leader with 38.79% of users who still prefer Windows XP. About a quarter of users in China (27.35%), India (27.52%), and Algeria (24.25%) also prefer this legendary system. Every fifth computer protected by Kaspersky Lab products and located in Italy (20.31%) and Spain (19.26%) runs under XP. With 4.52% the USA is bottom of this chart.

.

Using an outdated version of an operating system is fraught with the risk of cyber-attacks involving exploits, special programs that target vulnerabilities in legitimate software to infect a computer with other dangerous malware. More information about this appears in the following chapters of the study.

Part 2: vulnerabilities and exploits

Exploits are one of the most effective tools to deliver "payload" – additional malware with various malicious functionality - to victim computers without users being aware of it. According to the Java under attack - the evolution of exploits in 2012-2013 survey conducted by Kaspersky Lab last year, the most popular exploits target weaknesses in Java. This is due to the fact that this platform is the world's most widespread (according to the official figures, the Java software is installed on more than 3 billion devices) and it abounds in serious vulnerabilities found during the study period.

Windows OS, with built-in software like Microsoft Office and Internet Explorer, is one of the few products that can rival Java's audience reach. In addition, vulnerabilities are regularly found in Microsoft software which could theoretically prove that cybercriminals' exploits for Windows and other Microsoft products are popular.

Whether this is in fact the case will become clear from the following chapters

Microsoft vulnerabilities

According to Kaspersky Lab and data received from open sources[3], during the first six months of the year 161 vulnerabilities were found in 377 Microsoft products. The majority of them (113) were in Internet Explorer. 19 vulnerabilities were detected in Windows[4] versions and 11 vulnerabilities in Office (including Office Web App).

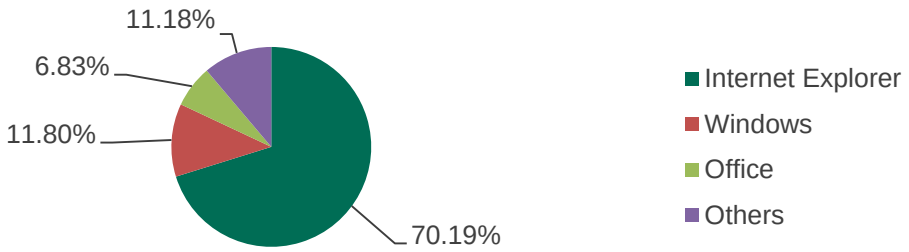

Fig. 10: Vulnerabilities in Microsoft products, first half of 2014

Noticeably, during the same period in 2013 the number of vulnerabilities detected in Internet Explorer, Windows and Office accounted for 55, 66 and 3 respectively.

[3] The study used data from http://www.cvedetails.com/ which integrates the information about all known vulnerabilities in popular software received from various open sources

[4] In this case, an OS vulnerability refers to a vulnerability in various technologies, services and protocols, which are integral parts of the specific Windows versions

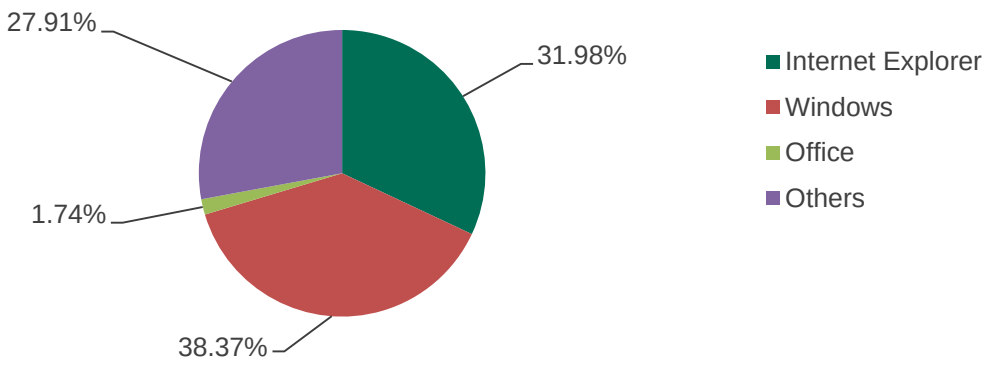

Fig. 11: Vulnerabilities in Microsoft products, first half of 2013

As you can see, there has been much shift during the year. Although we saw almost the same total number of vulnerabilities uncovered (172 in the first half of 2013 against 161 in the first half of 2014), the distribution of vulnerabilities between the key Microsoft products has changed significantly. The number of vulnerabilities in various versions of Internet Explorer doubled while the amount of vulnerabilities in the OC and its components dropped nearly threefold. This decline was caused by Windows XP. A year ago, IT security experts actively tested the system and found 46 vulnerabilities during the first 6 months of 2013 while over the same period in 2014 a total of 6 vulnerabilities was detected. This reduction, however, hardly means that Windows XP has run out of vulnerabilities. The fact is that the most notifications about vulnerabilities in Microsoft products are published by Microsoft, and the end of XP support means the end of safety testing.

Throughout Windows XP's entire existence 727 different vulnerabilities were detected. This is the all-time record among Microsoft operating systems. For comparison, up to now 467 vulnerabilities have been found in Windows Vista, which was released five years after XP, 465 vulnerabilities were found in Windows Server 2008, 338 vulnerabilities in Windows 7, 78 vulnerabilities in Windows 8 and 22 vulnerabilities in Windows 8.1.

However, a large number of vulnerabilities does not mean they are all used to create exploits and successful attacks. Cybercriminals are most likely to exploit vulnerabilities which don't need any special conditions, or which offer particularly dangerous opportunities to execute malware on the compromised computer. This malware is usually designed to steal money or confidential data, or for other illegal activities.

Exploits for vulnerabilities in Microsoft products: far behind the leaders

During the period from November 2013 to June 2014 Kaspersky Lab recorded a total of 15.06 million identified[5] exploit detections on 3.64 million computers running under different Windows versions. As expected, most of these detections (52.85%) involved exploits written for Java vulnerabilities. Exploits for various Microsoft products (Office, WMA, Visio, Silverlight) are much less popular with just 1.67% of detections.

Although during the reporting period Kaspersky Lab detection systems identified exploits for more than 40 vulnerabilities in Microsoft products, the main "contribution" came from only four of them.

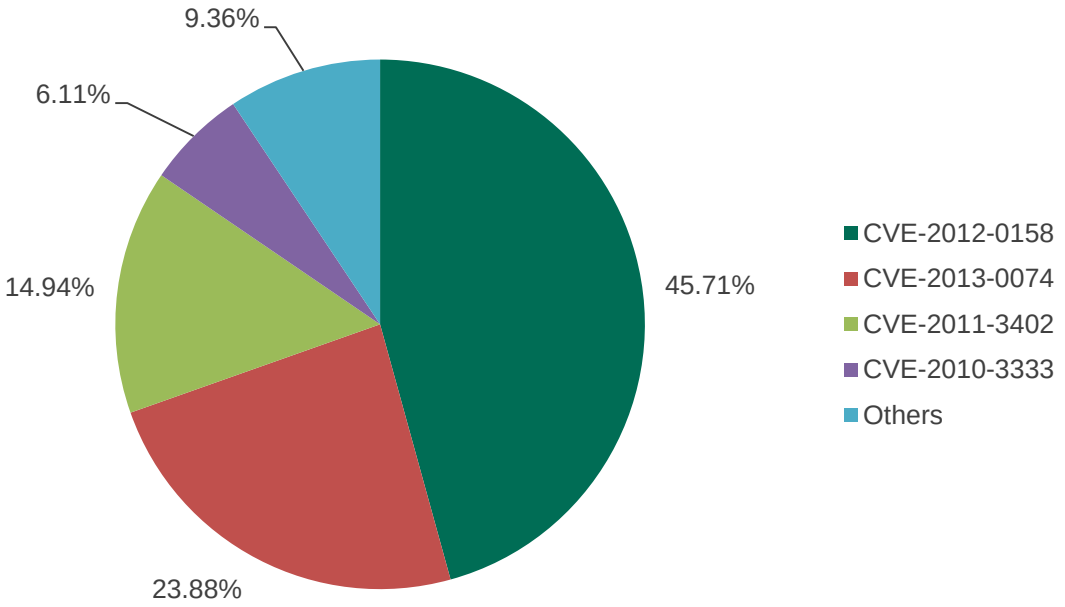

Fig. 12: Detections of exploits for Microsoft products, November 2013-June 2014

As the graph shows, the majority of detections involve the CVE-2012-0158 vulnerability in Microsoft Word. It first appeared in October 2012, and in early 2013 Kaspersky Lab experts reported an exploit for this vulnerability was used by Red October operators. Later, exploits for this vulnerability were seen by Kaspersky Lab experts in yet another cyber-espionage campaign - Nettraveller – and many other attacks. By the way, 6.11% of the total number of detections of exploits for Microsoft products involved CVE-2010-3333, a well-known Word vulnerability used in combination with CVE-2012-0158 in both Red October and Nettraveller.

[5] Identified exploits in this case refer to the exploits where it was possible to identify the software platform for which they were written. For technical reasons, part of Kaspersky Lab's detections is made using common heuristics methods. These methods cover various types of exploits but do not allow us to accurately determine the platform targeted by the exploit. Data about these detections was not included in this study

Second in popularity were the exploits for the CVE-2013-0074 vulnerability in Microsoft Silverlight, an application that displays multimedia content. This technology has not matched the popularity of its rival, Adobe Flash, exploits for this vulnerability were used by cybercriminals. Specifically, in autumn 2013, more than half a year after Microsoft released a security update to patch this vulnerability, an exploit for it was detected as part of the Angler exploit pack and was used throughout the study period.

CVE-2011-3402 came third with 14.94% of detections. This vulnerability in the TrueType fonts processing module affects a number of Windows versions (from XP to Windows 7 including Windows Server 2003/2008). It was detected in September 2011. Malicious applications for its exploitation were also used to spread the dangerous Trojan Duqu spyware, which has sibling connections with the infamous worm Stuxnet. Incidentally, it is closely connected with the another vulnerability that often threatens Kaspersky Lab users.

The echo of Stuxnet

The summer of 2010 saw the appearance of Stuxnet, a computer worm which, as it turned out later, had been designed specifically to sabotage the uranium enrichment process at several factories in Iran. Stuxnet was a real sensation which demonstrated what malware was capable of when precisely targeted and rigorously prepared. To proliferate, the worm used the exploit for the CVE-2010-2568 vulnerability. It is an error in processing shortcuts in Windows OS enabling the download of the random dynamic library without the user's awareness. The vulnerability affected Windows XP, Vista, 7 as well as Windows Server 2003 and 2008.

The first malware exploiting this vulnerability was registered in July 2010. Specifically, the worm Sality uses this vulnerability to distribute its own code: the worm generates vulnerable shortcuts and distributes them through LAN. Should a user open the folder containing such shortcut, the malicious program immediately begins launching. After Sality and Stuxnet this vulnerability was used by the well-known Flame and Gauss spyware.

In autumn 2010, Microsoft released a security update which patches this vulnerability. Despite this, Kaspersky Lab detection systems are still registering tens of millions of detections of CVE-2010-2568 exploits. Specifically, over the period of study more than 50 million detections on more than 19 million computers worldwide were recorded.

We deliberately did not consider the statistics of these detections: due to the way in which this vulnerability is exploited it is impossible to determine the cases in which Kaspersky Lab products protected from real attacks using exploits for CVE-2010-2568 and in which just detected automatically vulnerable tags generated by a worm.

Nevertheless, KSN statistics allow us to make certain conclusions. For example, the graph below shows the dynamics of Kaspersky Lab detections of exploits for the CVE-2010-2568 vulnerability and the Sality virus.

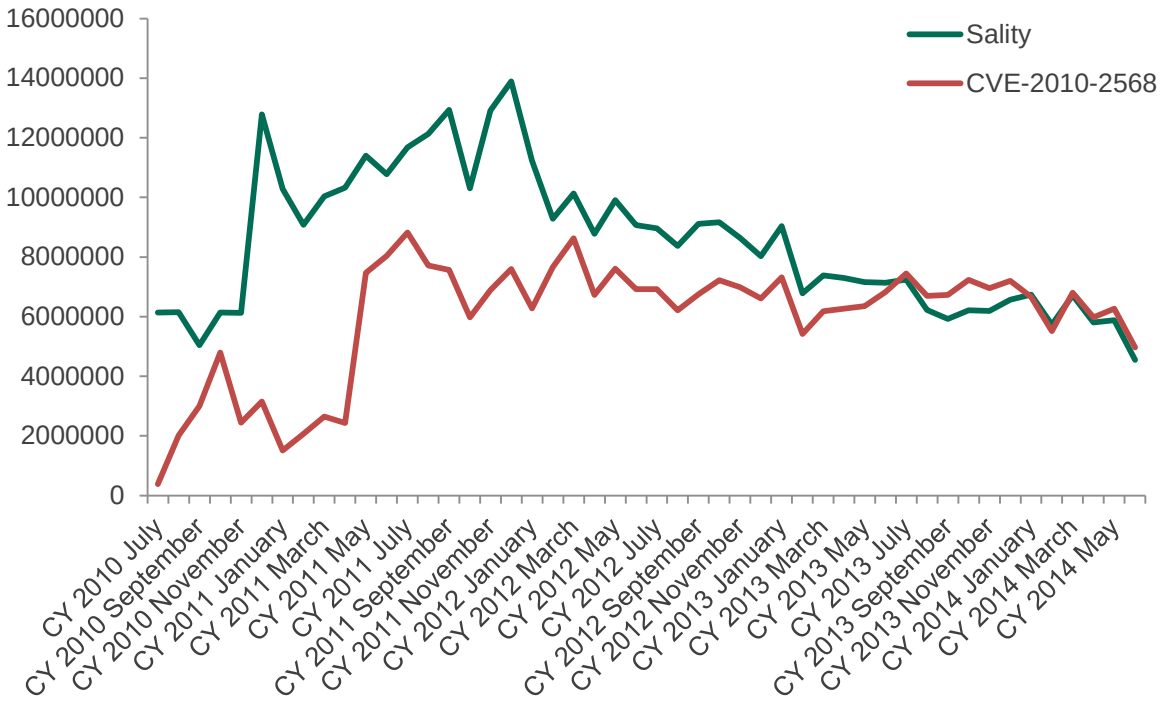

Fig. 13: Sality and CVE-2010-2568 detections

As is seen from the graph, the relationship between these two malicious programs has endured for many years. The decline in the number of detections for these two malware families is primarily due to the reduction in the number of Sality modifications. It is obvious that since January 2014 the number of Sality and CVE-2010-2568 detections has almost synchronized which confirms that only the version working in combination with CVE-2010-2568 remained active during this period while previously many other versions of malware were widely spread.

It’s worth noting the distribution of computer operating systems on which detections of the exploit for LNK vulnerability were registered. The lion's share of detections (64.19%) registered over the last eight months involved XP and only 27.99% were on Windows 7. Kaspersky Lab products protecting server operating systems Windows Server 2003 and 2008 also regularly report detection of these exploits (1.58% and 3.99% detections respectively). The large number of detections coming from XP users suggests that most of these computers either don’t have an installed security solution or use a vulnerable version of Windows - or both. The detections coming from server systems prove the presence of malicious shortcuts exploiting the CVE-2010-2568 vulnerability on network folders with open access.

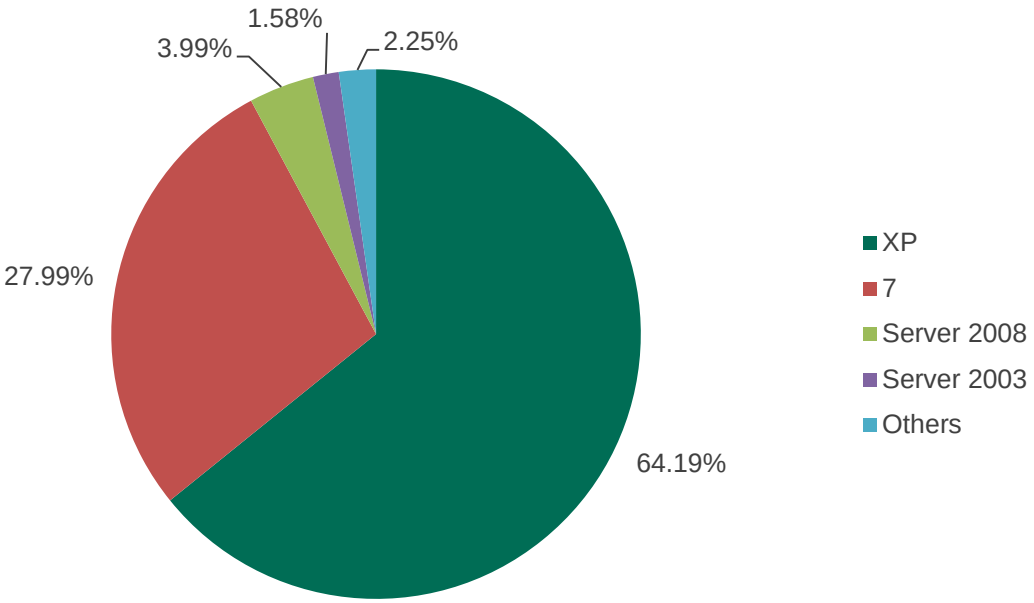

Fig. 14: CVE-2010-2568, OS distribution

The geographical distribution of all registered CVE-2010-2568 detections is also interesting.

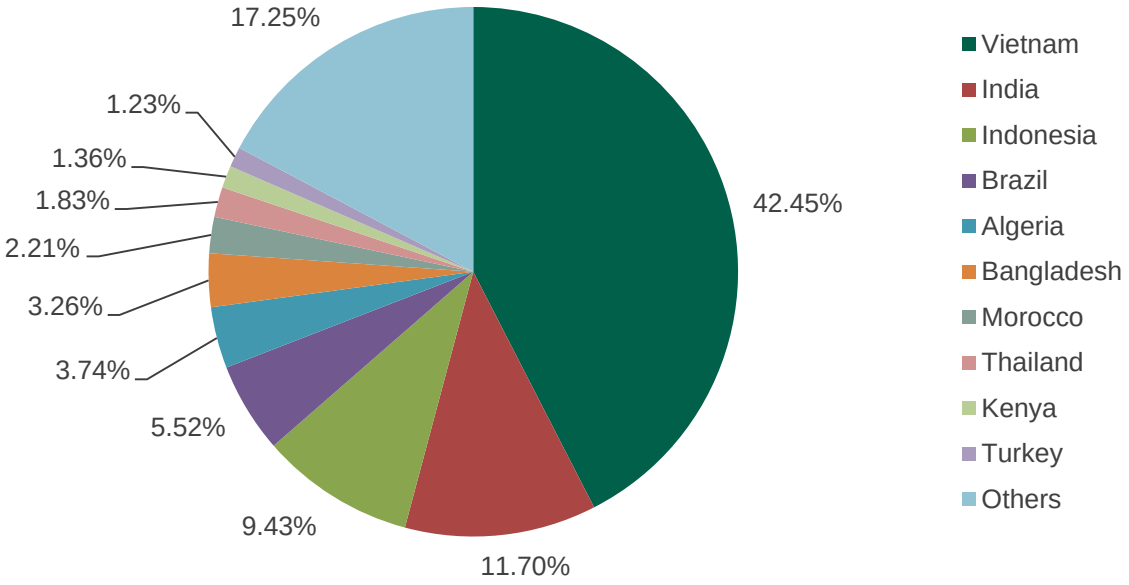

Fig. 15: CVE-2010-2568 detections, country distribution Nov 2013 - June 2014

As is seen, Vietnam (42.45%), India (11.7%) and Algeria (5.52%) are among the leaders not only in the percentage of outdated XP users but also in the number of Kaspersky Lab detections of one of the most dangerous Windows vulnerabilities currently known.

It should be mentioned that these figures by no means prove that users in countries with the biggest number of CVE-2010-2568 detections are all using vulnerable Windows versions. For technical reasons, KSN does not provide the opportunity to determine exactly which security updates are installed on each computer. However, some indirect factors such as the geography of detections and the distribution of operating systems help us to spot countries where users should think about the security of their computers. Cybercriminals are usually self-seeking and do not do things that do not give profit. Perhaps that is why the countries with the small proportion of computers running under XP, such as the USA, Germany, the UK, Canada, etc., are not included in the charts demonstrating the distribution of CVE-2010-2568 exploits simply because using this vulnerability to distribute malware in these countries will not be effective.

Conclusion and recommendations

The main conclusion of the study is the following: nearly 13 years after its launch, Windows XP is still running on the computers of a significant number of users worldwide, and it is obviously a big threat to the security of the users.

The second important conclusion is: although exploits for Windows and other popular Microsoft products are not widespread (except for LNK vulnerability CVE-2010-2568) compared with, for instance, exploits for Java vulnerabilities, they constitute a great threat and examples of exploiting Windows and Microsoft Office vulnerabilities in complex cyber-espionage campaigns is further proof of this.

The third conclusion is: when it comes to Windows and other Microsoft products vulnerabilities, the attackers are not willing to "keep up with the times" and create exploits for relatively new vulnerabilities. This might happen because the attackers are quite satisfied with the old vulnerabilities - a large number of computers with outdated Microsoft software boost the efficiency of exploits for well-known vulnerabilities.

To avoid potential information security incidents caused by the non-updated Microsoft software and their negative effect, Kaspersky Lab experts recommend the following:

For home users:

- Use the latest Windows version and monitor notifications about the appearance of security updates for it and other Microsoft products
- Unfortunately, even an experienced user can be confronted with the situation when the vulnerability already exists but the patch for it does not. Therefore, to ensure the highest possible level of protection for your digital valuables, use a security solution incorporating the technology to combat exploit-based attacks.

For corporate users:

The popularity of LNK exploits in Windows, as described in Chapter 2 of this study, illustrates the fact that many network administrators - including corporate network administrators - do not pay enough attention to the public servers under their control. As a result, malicious software such as Sality has been self-reproducing in local networks for years, jeopardizing the users who access them. Non-protected workstations running under a vulnerable version of Windows may become the entry point for a targeted of attack on the company. Therefore, Kaspersky Lab encourages companies to carefully monitor the software used on their corporate servers and workstations and to avoid any false economies when protecting them from malicious attacks.

When migrating to the most recent version of the operating system is not possible for technical reasons, it is necessary to use a reliable security solution that integrates the

tools to prevent exploit-based attacks and to detect and quickly patch vulnerabilities in corporate software.