International Journal of Multidisciplinary Research and Development
Online ISSN: 2349-4182, Print ISSN: 2349-5979; Impact Factor: RJIF 5.72
Received: 20-11-2019; Accepted: 21-12-2019
www.allsubjectjournal.com
Volume 7; Issue 1; January 2020; Page No. 110-114

Status of Microsoft windows operating system from security perspective in Afghanistan

Rafiqullah Baryalai
University of Sayed Jamaluddin Afghani, faculty of Computer Scienc, Asadabad, Kunar, Afghanistan

Abstract
High usage of pirated software in developing countries like Afghanistan is very common. Overlooking copyright and its legal obligations is among several issues that encourages usage of pirated software. Microsoft Windows is used highly in Afghanistan. The survey conducted for compilation of this article shows high percentage of pirated copies being in use today. Users often underestimate the value of a genuine Microsoft Windows copy while ignoring several security threats and risks they are prone to for using pirated software products. Research has proven that most of pirated software come with malware, Trojan Horses, and security bugs that opens back doors for hackers to penetrate into systems.

Keywords: Microsoft windows, security, pirated software

Introduction

Usage of pirated software is an issue known globally. Everywhere, people are trying to get hold of pirated copies with different motivations. Users could obtain a pirated copy from several online portals as well as many peer-to-peer networks [11, 12]. In countries well knowns for copyright violation, it is even possible to obtain a pirated and cracked copy of any software in counterfeit packaging in the shop around the corner for prices as low as one Euro per CD/DVD and Afghanistan is no exception in this regards.

Users and companies that are using pirated software are normally overlooking several important issues. They are spending more money and time on trouble shooting [13] their IT systems often gets failures and crush due to usage of pirated software. Studies on 600

Chinese companies show the usage of pirated Microsoft Windows sever, where most of them agree on loosing time and money in restoring company date due to regular crushes of their operating systems [11].

Pirated software do not stop at just bringing loss in money and time. Test results from several studies by IDC (International Data Corporation) and partners on pirated software show malware, Trojan Horses and back door codes being associated with those software

These malware codes are not just integrated into the software, but also transmitted to user's computers as soon as they are visiting websites they wish to get the tools and software products from. In many cases hackers lure their victims into using those products by offering them counterfeit software [11, 12, 13, 14].

Usage of pirated software is not necessarily limited to just operating systems in Afghanistan. Users obtain pirated copies of their software; be it a simple image processing tool or a security software such as Anti-virus software. This paper has only touched the usage of pirated operating systems with a focus on Microsoft Windows operating system. The data collection is done through online and printed distribution of questionnaires. A total of 1032 people took part in the survey from around the country including 27 participants from other countries around the world. The results of data analysis was limited to only respondents from Afghanistan that left us with 1005 participants. As a result of this survey, Microsoft Windows seems to be highly used in the country (93.1 %) with a 46.4 % of pirated copies being used. Lack of awareness about legal, security and privacy issues of a pirated software is another major finding of this survey.

Operating Systems

A computer is a set of various hardware components built together to carry out tasks provided by user applications. However, if every programmer had to write their own pieces of code for communicating with these hardware components, also called Physical Resources [1], they would be ever stuck dealing with this primary task of communicating. To simplify this task and let programmers write more useful applications as well as to automate the resource management procedure, Operating Systems came to existence. For a paper essentially dealing with an Operating System, abbreviated as OS, it is worth explaining the reader what it is first. Operating System is a set of multiple small software, depending on the architecture [1] that acts as an intermediary manager between user application programs and the physical resources of a computer. Furthermore, it allocates each resource to the requesting user processes and should the resource be unavailable, the requesting process is scheduled, using one of many existing scheduling algorithms, to wait until the resource is free again. All the related mechanisms make the study of Operating Systems, Design, and Implementation an interesting topic. In simple words an Operating System is a manager who is supposed to provide the required resources that are requested by user application processes and should those resources be busy use certain scheduling mechanisms so that eventually the requesting processes can get and use the required resource [1, 2].

There are different types of computers in use around the world today. From super computers to mini devices such as smart phones and e-gadgets. All these machines have hardware resources and designed and built to achieve certain goals, therefore, it is of no big surprise to have an operating system on each of these machines. This paper only examines

the usage of operating systems running on personal computers, (Laptops and Desktops), namely, Linux, Mac OS and Microsoft Windows with the main focus in Afghanistan. In order to find out about usage and user awareness on security aspects of Operating Systems in Afghanistan, a questionnaire was distributed where more than
1,000, mostly university and school students took part in the survey. It seems Microsoft Windows operating system has the highest number of users making 93.1 % of the total. The findings will be explained in details in the later section, but first a short introduction to famous operating systems is in order.

Mac OS

Apple Inc., introduced its Macintosh computers in January 1987 [3, 4] for the first time. The company has been ever since introducing its own series of operating systems' versions. However, the early distribution of Apple Inc. was called System 1 to 9 [5]. Steve Jobs, announced the arrival of their new Mac OS in 1997 and the first distribution of Mac OS 8.0 was out in the market. The most recent distribution of this operating system is Called "El Capitan", which is Mac OS version 10.11.3 [www.apple.com] at the time of writing this paper [3, 4].

Linux

Linus Torvalds, a student at the University of Helsinki, was fed up with the proprietary software solutions of his time. He thought of making his own operating system. He started with a Kernel and named it Linux. His kernel alone wouldn't have taken him anywhere, therefore he published his Kernel in 1991 under the open source software agreement [5, 6]. Torvalds based his work on the Open Source philosophy which dates back to 30 years earlier and wanted to offer a freely available academic version of UNIX so people could use, maintain and develop according to what they wish [6]. He started digging at POSIX standard definitions, and finally managed to offer his operating system to public. Linux has earned its popularity quite fast as compared to other operating systems. A huge community believing in open source software paradigm promote it around the world. The most recent statistics published by W3Schools [7], shows 5.6 percent of the world population are using Linux. This study was based on usage data collected between 2003 and December 2015 through the www.w3schools.org website [7].

Microsoft Windows

Bill Gates and Paul Allen, in 1975 established Microsoft as they saw Personal Computers having a potential future. In a business meeting with IBM, they propose creation of an operating system that would manage the computer hardware and be a platform for many other application programs in 1980. They called it MS-DOS [8].

Since MS-DOS had a text based command line interface, Microsoft introduced the first version of its Graphical User Interface and named it Windows 1.0. [8]. This was a new initiative where instead of just typing in commands in a text based environment, users could use a mouse to click and work in a graphical interface. Throughout the years, Microsoft released various versions and made different architectural, security and usability extension and innovations at each version. The following years Microsoft introduced Windows 2.0 (Dec 1987), Windows 3.0 (May 1990), Windows NT (Jul 1993), Windows 95 (Aug 1995), Windows 98 (Jun, 1998) and Windows Me (Sep 2000) to the market [8]. Windows 98 was the last of the DOS based operating systems of Microsoft. Windows XP (Oct 2001), Windows Vista (2006), Windows 7 (2009), Windows 8 (2012), Windows 8.1 (2013) and finally Windows 10 (Jul 2015) [8, 9]. Microsoft claims Windows 10 to be one of its best and most complete operating systems ever and has a hope to have one billion users have installed Windows 10 by 2018 [8].

Microsoft Windows has split the User and Kernel area for better security and data protection for process management. The operating system is constantly switching between User mode and Kernel mode, as a security measure for data protection and prevention of probable loss of data over simultaneous usage of resources by similar processes. The following figure is a simplified version of the Windows Operating System's architecture design.

As seen in the figure above, the architectural view separates the operating system into two modes. The Kernel mode and the User mode. The User mode threads execute in a protected address space. Therefore, all the components shown above the dividing line get their own private address space. Making it safe for applying data protection policies and mechanisms [10].

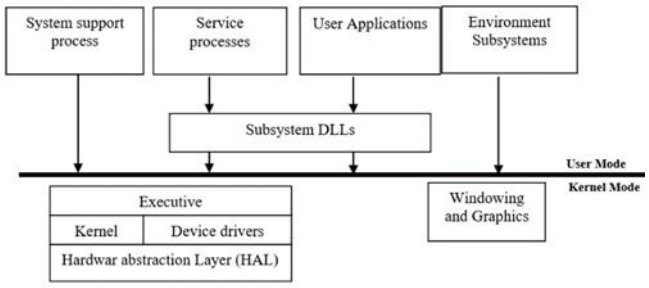

Fig 1: Simplified Windows architecture view Source [10]:

Following is a short explanation of boxes in the User Mode [10]:

- "Fixed (or hardwired) system support process, such as logon process and the Session Manager that are not Windows Services.
- Service processes that host Windows services, such as the Task Scheduler and Print Spooler services" [10].
- User applications [10].
- "Environment subsystem server process; which implement part of the support for the operating system environment or personality presented to the user and programmer [10].

One of the mechanisms in Windows architecture is that user applications cannot call native Windows operating system services directly. The call should go through one or more subsystem dynamic-link libraries (DLLs). These DLLs act as a translator for user calls to native process [10].

On the Kernel side of Windows the following main components of the diagram is a following [10]:

- "The Windows executive contains the base operating system services, such as memory management, process and thread management, security, I/O, networking and interprocess communication.

- The Windows kernel consists of low-level operating system functions, such as thread scheduling, interrupt and exception dispatching, and multiprocessor synchronization. It also provides a set of routines and basic objects that the rest of the executive uses to implement higher- level constructs
- Device drivers include both hardware device drivers, which translate user I/O function calls into specific hardware device I/O requests, as well as non-hardware device drivers such as file system and network drivers.
- The hardware abstraction layer (HAL) is a layer of code that isolates the kernel, the device drivers, and the rest of the Windows executive from platform-specific hardware differences.
- The windowing and graphics system implements the graphical user interface (GUI) functions, such as dealing with windows, user interface controls and drawing." [10].

Risks of Pirated Software

IDC, International Data Corporation, studies the risks and security issues of pirated software regularly. There are several papers available on recent studies being carried out by IDC and partners in the countries well known to using pirated or counterfeit software. In one of the papers published on microsoft.com "Risks and Hazards of Pirated Windows Sever", IDC believes [11]: "Enterprises face substantial security risks when using unlicensed or pirated software. The risks range from damage to their IT systems, impairment of business operations, to reputational damage." [11]. Some 600 enterprise around China were surveyed in this study and the finding is quite interesting. The survey participants mostly believe pirated software would miss key features, they found embedded viruses and Trojan Horses; financial and time loss on data recovery upon occurrence of a security breach, under estimating consequent legal and public embracement of using pirated software as well as they agreed on the the potential security risks of such software could outweigh the savings of purchasing a legal copy, are summary of the finding of this study [11].

Research has proven that a pirated software frequently has malicious codes. Most of pirated Microsoft products either do not contain a license key or use a "cracked file" to bypass the key and activation processes [11]. You can obtain a copy of these software, in counterfeit packagings in Software stores in Afghanistan with a prices as low as one Euro. All these software are cracked and also used by enterprise. A telecom company in Kunar Afghanistan, used a pirated copy of Microsoft Windows Sever 2008 to manage the internet-sharing between some of its customers and offices.

Another study by Gantz et.all from IDC audited websites that offer pirated software, key generators and counterfeit products. They visited those websites, downloaded tools and tested them [12]. In this study, they found that with simple web search users are directed to those websites. Some 25 % [12] of the websites they visited during the study tried to install malicious or unwanted software. In this study they also found that the tools they download from 11 % [12] of the websites as well as 59 % [12] of the peer-to-peer networks contained malicious or unwanted code fragments. In this study they also confirm that offering of counterfeit software, key generators and pirated Windows operating systems are just another way for hackers to lure their victims in using them and through that gain access over their data [12].

IDC and National University of Singapore, in a joint study in 2014 carried across 11 countries around the world, found a 33 % [13] chance of encountering malware, when a pirated package is installed. Some 61 % of the total number of PCs that were inspect by this study in 11 countries, were infected with malware [13]. According to this study, the Asia Pacific region will incur more than 40 % [13] of the worldwide consumer losses and more than 45 % of enterprise losses due to usage of malware and pirated software [13].

Although, Afghanistan was never part of this study, but the survey conducted by the author, shows similar results in Afghanistan to be affected by similar losses. Any simple software related issue is solved by fresh installation of a pirated copy of Windows operating system all the time. Braskamp and Soffronoff [14], did a comparison between Microsoft Genuine products and their Pirated counterparts and the presented results makes the reader wonder why people don't use genuine products? Similar question was kept in mind when writing this article and the answer will come in the related case study section.

Braskamp and Soffronoff [14], evaluated and compared both types of software in terms of Performance, Productivity, Power Consumption and Battery life; regardless of the security risks that pirated software can leave the user with, their results are still interesting. They have proven that users experience superior performance as compared to those who use counterfeit products. Genuine Microsoft Windows boots faster [14], which makes sense, since the pirated counterparts are busy loading some malware and Trojan horses during the load time of the operating system. They tested the genuine and pirated copies of Microsoft products on Intranet, popular heavy webpages and recorded the loading time; performance and productivity seemed to be higher and better in the genuine copies as compared to their counterfeit counterparts [14]. The paper also has the methodologies for running the tests on each test item they have used.

Discussions and Results

Afghanistan is a country where copy right laws cannot be enforced easily. Computers and smart phone usage have had a rapid growth in the last 10 years. People, tend to use computers more on a daily basis and small businesses are getting interested in using computers to record their transactions. Despite all the infrastructure issues such as lack of stable electricity, this phenomenon has been something of interest to people lately.

As the main goal of this paper was to evaluate the usage of Microsoft Windows operating system from legal and security perspective, it was decided to collect data from local people. A survey in the form of questionnaire was designed and put online for public to access. However, as lack of interest in contributing to research is another common issue one faces in Afghanistan a lot, the total number of people who took the online survey were

257 during one month, 27 of which were people from other countries. I shared the link to the online survey on my Facebook wall, where the number of likes this post received were three times more than the number of forms that were filled out. One could easily argue that people tend to use internet for checking Facebook quite often. More participants were needed, we switched to the old school paper based questionnaires. The printed questionnaires were then distributed among students at the university and schools as well as random Internet-Cafés in Kunar city. After a

period of two months, we managed to have 1032 questionnaires. The none Afghan participants of the survey were excluded from the statistics and the results reflects the opinion of 1005 persons in total from Afghanistan.

This survey covered the basis for understanding which operating system is commonly used as well as usage of counterfeit and pirated software in the country and people's awareness about security breaches that could be caused by those kind of software. Security updates and what they meant to them and why they were using the operating system they were using to no surprise, 93.1 % of the correspondents said they had Microsoft Windows installed on their computer, while Mac OS users stayed second and Linux users stayed third 6.7 % and 5.0 % respectively. Wither their operating system was registered or a cracked copy, 46.4% responded with their operating system being a pirated copy, while 21.5 % had no idea what it meant for a software to be genuine. Security updates being provided by operating system vendors seemed to be a confusing item of the survey; 70 % of the correspondents replied with either they didn't know what a security update meant or they choose disabling them as their pirated copy would get caught. A conflicting fact found during this survey was people's interest in having access to regular updates. A total of 59.8 % of correspondents said it was important for them to have access, while this number is in conflict with the number of pirated software users.

Another purpose this questionnaire served well was finding people's awareness on issues, such as security awareness, technical details of a software, the state of a software being genuine, counterfeit or pirated. The "I don't know" option, in exact or similar words was integrated in the list of options for five questions of survey which was to find out if the correspondent knows about issues such as security and pirated or cracked software. An average of 21.1 % of correspondents lacked awareness on security and legal issues of software they were using.

The facts are on the table. People use computers and most of them have a Microsoft Windows Operating System installed. Around half of them are using pirated distributions of the operating system. The following four points are a summary to why people still tend to use pirated copies.

- Lack of awareness about copyright and its legal standpoints. The copyright is never enforced anywhere in the country, be it an individual or an enterprise. There is no consequences for the usage of illegal software products.
- The country's 31.63 million population has a GDP of 20.04 million US Dollars [15]. "Low income" economy [15] is another factor that people overlook obtaining legal copies of Microsoft products, despite its popularity in usage. A second hand Dell Latitude D620 [16] laptop, still popular in the market, is sold for nearly 150 US Dollars. If a person buys that laptop, he never thinks of paying for a legal version, he simply can't afford it.
- Getting a pirated copy of any product is easy. Several software shops are in the market selling CDs and DVDs with all the cracking tools in counterfeit packing. You need to pay less than a Dollar to obtain one. "Your machine is not working, do a fresh installation of Windows. It will be fixed", is a popular quote among many people who offer computer repair services in the market.
- Lack of security awareness. People who use pirated software products don't know about their security risks and the harm they can cause to their data and privacy.

The only solution to these issues is Education. Educate people about copyrights, security issues and all the consequences that pirated software can have. Raising security awareness in terms of cracked software and all its attached problems is an important step to be taken. Schools and universities can play a crucial role in informing and educating people about the risks.

Another alternative is promoting open source and free software in the country. It doesn't seem to be a difficult task. There are many Android users already. They are using an open source operating system. As for having a Linux operating system 5.0 % of the correspondents of the survey have replied positive and 8.8 % of the correspondents have claimed Linux being their favourite operating system. Although, this is a very low percentage, but a "journey of 1000 miles starts with one step". This shows there is some awareness. It should be promoted and people should get more training to use it. However, a more broader study and analysis of the society on usage of computers, smart phones, pirated or legal software is required to find out more details on this issue and be able to make a proper judgment on the status of the pirated software and their related risks in the society.

References

1. Stallings William. Operating System: Internals and Design Principles; 7th Ed, 2011.
2. Tanenbaum Andrew. Modern Operating Systems; 3rd Ed, 2007.
3. Singh, Amit; A Brief history of Mac OS X; Mac OS X Internals, 2003. URL: http://osxbook.com/book/bonus/ancient/whatismacosx/ history.html (Last Accessed: 24 Feb 16, 13:00).
4. Warren, Christina. The Evolution of Mac OS from 1984 to Mountain Lion; Mashable, 2012. URL: http://mashable.com/2012/02/17/ mac-os-timeline/#2_cwknFhLqqx (Last Accessed: 22 Feb 16; 13:00)
5. Torvalds Linus. Diamond David. Just for Fun: The Story of an Accidental Revolutionary; Harper Business, 2002.
6. Garrels Machtelt. Introduction to Linux: A Hands on Guide; TLDP, 2008. URL: http://tldp.org/LDP/intro-linux/html/index.html (Last Accessed: 24 Feb 16, 13:00
7. W3Schools.com; what is the Trend in Operating System Usage? W3Schools; URL: http://www.w3schools.com/browsers/ browsers_os.asp (Last Accessed: 24 Feb 16, 13:00).
8. Microsoft Inc., A History of Windows; Microsoft, 2015. URL: http://windows.microsoft.com/en-us/windows/history#T1=era0 (Last Accessed: 24 Feb 16, 13:00)
9. Egan Matt. Windows 10 release date, price and features; PC Advisors, 2016. http://www.pcadvisor.co.uk/new-product/ windows/windows-10-release-date-price-features-uk-fall-update-3496959/ (Last Accessed: 24 Feb 16, 13:00)
10. Russinovich Mark, Solomon David A, Ionescu Alex. Windows Internals; Microsoft Press; 6th Ed, 2012.

11. Microsoft Inc., Risks and Hazards of Pirated Windows Server; Microsoft, 2012. URL: http://download.microsoft.com/documents/china/gsi/WP_BSA_windows_server_SC_LORES_EN.pdf. (Last Accessed: 24 Feb 16, 14:15).
12. Gantz John F, Gillen Al, Christiansen Christian A. The Risks of Obtaining and Using Pirated Software; IDC, 2006. URL: http://download.microsoft.com/download/c/e/d/cedae44e-8191-4e64-953a-8769a0733d3b/IDCWhitePaper-RisksofPiratedSoftware.pdf. (Last Accessed: 24 Feb 16, 14:15).
13. Gantz John F. *et al*. The Link between Pirated Software and Cyber security Breaches: How Malware in Pirated Software is costing the World Billions; IDC, 2014. URL: https://news.microsoft.com/download/presskits/dcu/docs/idc_031814.pdf. (Last Accessed: 24 Feb 16, 14:15)
14. Braskamp Case, Roffronoff Jake. Genuine Microsoft Products vs. Pirated Counterparts; Harrison Group, 2011. URL: https://news.microsoft.com/download/archived/presskits/antipiracy/docs/genuinemsproducts.pdf. (Last Accessed: 24 Feb 16, 14:15)
15. World Bank; Afghanistan Data and Statistics, 2014. URL: http://data.worldbank.org/country/afghanistan (Last Accessed: 24 Feb 16, 14:15).
16. CNet; Product Reviews; Dell Latitude D620 First Take; Apr, 2006. URL: http://www.cnet.com/products/dell-latitude-d620/ (Last Accessed: 24 Feb 16,