المجلة الإلكترونية الشاملة متعددة التخصصات
العدد الثاني والثلاثون شهر (١) ٢٠٢١

# The impact of malware detection systems for mobile phones

**Mohammed Mualla Alharbi**

m.alwafi.1987@gmail.com

Information Security Specialist

## Abstract:

Knowing malware is the first step to protecting the phone from attacks. Most malware can be avoided. Malicious programs are special programs whose mission is to disrupt the system and sabotage its processes in addition to sabotaging data and information on the phone device, and it can be said about software that makes money illegally that it is Malicious software, and these programs can perform deletion and encryption operations so that the user cannot access his data and files without paying money or he may not be able to obtain them at all

Malicious malware attacks the phone in the form of viruses, worms, Trojans, spyware, adware or rootkits, and their tasks are often aimed at accomplishing illegal tasks such as stealing protected data, deleting confidential documents, or adding programs without the user's consent.

**Keyword: malware, detection systems, mobile phones, malware for mobile phones.**

**ملخص البحث:**

إن معرفة البرامج الضارة هي الخطوة الأولى لحماية الهاتف من الهجمات. يمكن تجنب معظم البرامج الضارة. البرامج الخبيثة هي برامج خاصة مهمتها تعطيل النظام وتخريب عملياته بالإضافة إلى تخريب البيانات والمعلومات الموجودة على جهاز الهاتف ، ويمكن القول عن البرامج التي تربح أموالاً بشكل غير قانوني أنها برامج ضارة ، ويمكن لهذه البرامج أن تؤديها عمليات الحذف والتشفير بحيث لا يتمكن المستخدم من الوصول إلى بياناته وملفاته دون دفع أموال أو قد لا يتمكن من الحصول عليها على الإطلاق

تهاجم البرمجيات الخبيثة الهاتف في شكل فيروسات أو فيروسات متنقلة أو أحصنة طروادة أو برامج تجسس أو برامج إعلانية أو برامج rootkits ، وغالبًا ما تهدف مهامها إلى إنجاز مهام غير قانونية مثل سرقة البيانات المحمية أو حذف المستندات السرية أو إضافة برامج دون موافقة المستخدم.

**الكلمات المفتاحية** : البرمجيات الخبيثة ، وأنظمة الكشف ، والهواتف المحمولة ، والبرمجيات الخبيثة للهواتف المحمولة.

## Introduction:

The mobile phone, a great invention that brought about a tremendous revolution in the world of communication, made the process of communication smooth, made it available and possible at any time, and made the privacy of calls between people a large space, especially since mobile phone communication is not only by voice calling, but by text messages and many more. Applications, so the mobile phone is like the personal computer that accompanies its owner everywhere, and no one can dispense with it if he wants to contact the whole world and know all the news first hand (Blake, H., 2008).

The mobile phone brought about a great qualitative leap in people's lives, as it allowed its users the freedom to communicate with everyone without being forced to stay at home. Before its invention, people were forced to stay next to the fixed phone while waiting for a call, but after its invention, mobility in all places became available and not Waiting for calls is a hindrance for the person, as the phone accompanies the person wherever he goes. This is why the mobile phone has become, at the present time, a necessity that a person cannot imagine his life without (Moberg, Å., et al, 2014).

It has become natural for each person to have his own personal phone and his own number that you can communicate through at any moment, so the best description that can be given on a mobile phone is that it is a personal companion to its owner, at the present time the number of mobile phone companies is very large, and they are all competing to make a phone with privileges not found in any other phone, which is why mobile phones have developed at a tremendous speed (Funk, J. L., 2004).

A mobile phone is considered to be a phone device that makes calls through the use of cellular network technology so that it is able to send signals to a cellular network, smart phones are a type of mobile phone, but it has the advantage of being an advanced device and has a touch screen, and the first mobile phone has been put up for sale. In 1984, its price reached nearly four thousand dollars, and statistics indicate that the number of mobile phones around the world reached in the year 2012 more than five billion mobile phones (Russell Ware, 2018).

Malware is a major problem that threatens the security of every mobile phone user. It is one of the most dangerous threats to a mobile phone and can steal personal information or hinder the functioning of the device. Malicious software includes various types of software, intended to cause system corruption or to access data without the user's knowledge (Hypponen, M., 2006).

Malware poses a major threat to computer networks due to the potential for heavy loss to the victim, most types of malware depend on some type of user action. Either you receive an email that requires you to download the exe file or there is a link waiting to click on it (Zyba, G., et al, 2009).

The attackers have a good knowledge of the vulnerabilities of various devices and exploit the weaknesses to reach their target, some malware can get onto your mobile phone by taking advantage of security vulnerabilities in your operating system and software. Older versions of browsers and their add-ons and components are considered easy-to-reach targets (Lawton, G., 2008).

Most of the time, malware is installed by users (you!) And ignore what they're doing and rush through software installations that include malware. Many programs install malicious toolbars, download assistants, a system and internet optimization tool, fake anti-virus software, and other tools automatically to harm the device (Peng, S., Yu, S., & Yang, A., 2013).

Therefore, it is imperative to detect malicious software to protect ourselves and our devices from falling into danger, as this research came with the aim of demonstrating the impact of malware detection systems for mobile phones.

## Problem Statement:

When downloading any application or file on a mobile phone, malware and malicious codes usually hide in fake versions of popular applications, without the user's knowledge of them, in addition to that these malicious programs are able to destroy the mobile phone, as well as have the ability to steal all data and personal information and fake it, which requires full awareness of these programs and how to deal with them.

## Malware software

Malware is an abbreviation of two words ("malicious software"): it means malicious programs and it is a programmatic code that works to harm the user, harm his computer, harm the computer network, or harm others, it also traces into or destroys the computer system without the consent of the owner. When malicious programs are installed, it is very difficult to remove them. Depending on the degree of the programs, their damage can range from slight annoyance (some unwanted advertising pages during the user's work on the computer) to irreparable harm that requires reformatting the hard drive, for example (Dunham, K., 2008).

They are special programs whose mission is to disrupt the system and sabotage its processes in addition to sabotaging the data and information on the phone, and it can be said that software for making money illegally is malicious software, and these programs can perform deletions and encryption operations so that the user cannot access his data and his files without paying money or he might not be able to get them at all (Qamar, A., Karim, A., & Chang, V., 2019).

Malware is one of the many types of small programs that have become widespread and infected. Malware metaphorically is a direct virus relative, the malware does many bad things on your computer such as monitoring your e-mail or instructing your e-mail to send spam on behalf of other people (Kondakci, S., 2008).

It can be said that they are insidious programs that secretly install themselves on your phone device, perform secret operations without your permission, as these malwares do hundreds of things from your phone device such as recording the keystrokes that you press, stealing your passwords, monitor your browser usage, open new browser windows on its own, send email using your personal mail, redirect your browser to specific pages, and report your personal information to remote servers.

One of the most popular ways to get malware is the Internet and e-mail. This software may reach you by browsing to a site that previously seized it, downloading unsafe files, opening dangerous e-mails or by clicking on any of the untrustworthy ads and profit messages Suspicious (Hypponen, M., 2006).

## Methods for detecting exposure to a malicious program:

Mostly, it is the abnormal malware behaviors that reveal its presence, so it is done through the following things (Bayer, U., 2009) & (Grégio, A. R. A., et al, 2015):

1- Unusually slow operation of the device, this is noticeable in normal mobile phone use cases.
2- The appearance of advertisements on the screen in places where they do not usually appear frequently, it is one of the most correct indications of the presence of malware, so you can usually find it in the form of a profitable advertisement such as Congratulations You won a million dollars.
3- Sudden system halting, blue screen, and freezing, especially on Windows devices, after encountering major errors as a result of malicious software. If the disk storage space is mysteriously lost, this is an indication of the presence of a large size of harmful files within the computer.
4- Strange increase in internet usage in the device.
5- The increased use of system resources as well as the fan starting up too quickly is a sign of malware activity in the background.

6- Change the home page in the browser without permission, and clicking on the links leads to incorrect and unwanted destinations, this also may slow down the browser.
7- Unexpectedly new components and tools or extensions within the browser, which is dangerous for the browser.
8- Antivirus software has stopped working and the user is unable to update it.
9- There is software that shows itself directly and informs the user that it has managed to obtain this user's data, and he must pay money to be able to retrieve it.

Even if the computer is working well and you did not notice any strange behavior, this is not sufficient evidence that the computer is healthy, but malware can hide in smart ways.

## Types of malicious programs:

### 1- Viruses:

It is so named because it resembles the natural viruses that infect the human body, which are characterized by their small size and greatness of harm, and the difficulty in detecting them, and the speed of their reproduction, in addition to the possibility of their transmission to other healthy bodies and infection, and these characteristics (Filiol, E., 2010).

It is a small program that adds itself to all the files that you want to contaminate, the goal of which is either to destroy certain data in the infected device, or to annoy the user by slowing down the operation of the device (Filiol, E., 2010).

It is a malicious program that, when loaded, attaches to another program and repeats itself and infects other programs.

Characteristics of viruses:

It is distinguished by its ability to reproduce significantly and contaminate a large amount of files and programs in the computer, and it is at this stage that it is in the process of spreading, but without any destruction, and the destruction may begin while the user is running one of the programs or files contaminated with this virus (Aycock, J., 2006).

The use of viruses and the methods of their spread it can be transferred to the user's device without his knowledge, through a file contaminated with a computer virus, or in the form of a mail message with an attached file contaminated with a virus, or through chatting sites where an interviewer asks you to receive a file and open it without knowing its content (Aycock, J., 2006).

Its damages range from destroying all the contents of the device and the occurrence of other problems, such as slow performance of the device, the emergence of error messages repeatedly, or automatic restart of the device, and that depends on the goal of the virus programmer from it, and the extent of the damage that he wants to inflict on the device (Bose, A., & Shin, K. G., 2006).

## 2- Trojans Horse:

It is a small program, that appears in the form of a file, pretending to be doing useful work, or making important updates to the device, and as soon as it is turned on it begins to destroy or spy directly without introductions. It is considered one of the most dangerous malware as it enters the computer illegally and collects financial and private data and allows modification to it and thus allows the installation of many ransomware programs (Zhang, X., & Tehranipoor, M., 2011).

A Trojan horse is distinguished by the fact that it does not multiply between files and programs and does not contaminate it like a virus, it destroys without an implementer, for months or years without knowing it (Bryce, T., 2006).

Often it is transmitted to the user's device with his knowledge, it may arrive through a file or program that the user brought from another person, either through storage media, or through a computer network, or in the form of a mail message with an attached file contaminated with a virus, or through chatting sites where it requests One of your interlocutors receives a file and opens it, which are in fact Trojans (Zhang, X., & Tehranipoor, M., 2011).

The damages of the Trojan horse range from the user's loss of data and information on the device to the violation of its privacy, some types destroy data and information on the device, or slow down the operation of the device and create many problems that lead to the collapse of the device (Fuentes, D., et al, 2010).

As for others, they spy for the account of their maker and programmer, and they send information that may be confidential, such as credit card numbers or passwords for postal accounts, and some can take pictures of the desktop that show what you are doing now and then send these pictures to its programmer, and some give The possibility of full control of the device as if it is in front of it, enabling it to delete and modify files, and therefore the damage may be many times greater than that of viruses (Zhenfang, Z. H. U., 2015).

## 3- Worms

it small programs, usually received via a computer or phone network, are often intended to annoy the user, or destroy the information stored in the device, in addition to causing large traffic to the network by sending and receiving large data continuously that may lead to the collapse of the network or its slowdown, so called because it is similar to natural worms in the speed of reproduction and spread (Chen, Z., Gao, L., & Kwiat, K., 2003).

They are dangerous programs that repeat themselves a lot as well as be ready to move to other devices and increase in them and cause destruction of files.

Worms are characterized by their small size and amazing speed of spread, they may infect millions of devices within a short period of time, due to their dependence on the computer network to spread, they have the ability to reproduce and spread, but they do not contaminate files or programs or add themselves to them, but rather they spread in the network that The contaminated device is linked to it, as its spread exceeds the device itself to reach others through the computer network (Pratama, A., & Rafrastara, F. A., 2012).

Worms are spread through the Internet or the local network, through a mail message with an attached file containing the worm itself, or through a security vulnerability in the operating system (Toutonji, O., & Yoo, S. M., 2009).

Worm damage is distributed between the user's device and the network to which this device is connected, as it may destroy the data in the device, or contribute to the slow performance of the device by consuming the device's resources without interest, in addition to making the computer a source of harm to others through the spread of other healthy devices. On the net it weighs down, by sending itself to as many postal addresses as possible (Weaver, N., et al, 2003).

In addition, some worms are designed to overthrow certain websites, as they flood the site from browser requests that lead to difficulty accessing the site or completely inaccessibility (Toutonji, O., & Yoo, S. M., 2009).

## 4- Bots: When Robots Control the World

They are automated programs that perform a specific process. There are many legitimate bots that help the Internet run smoothly, such as the Googlebot program. However, the bot can also be used to perform many suspicious operations such as infecting unprotected computers and adding them to a malicious bot network (botnet) (Wessel, M., et al, 2012).

The person responsible for operating the botnet can carry out many different types of attacks, by remotely controlling a number of computers. and for example. A bot can steal data from an infected computer, including user contacts, passwords, and other private information. Computers infected by the bot may also become mail propagation points, Spam, malware, and other nasty surprises to other users (Wessel, M., et al, 2018).

Finally, the bot can use the infected network to launch DDoS attacks and other attacks on a large scale. A bot is perhaps the most powerful type of malware, as it is able to spread in various ways and attack in many ways (Geer, D., 2005).

## 5- Spyware:

They are programs designed to collect your data and send it to a third party, without your consent or your knowledge. The data collected is sent to the app's creator or possibly to a third party, it can be stored in a way that can be recovered at a later time. Some spyware may monitor keystrokes ("keyboard recorders"), collect confidential information (passwords, credit card numbers, PIN numbers, etc.), collect email addresses or track your browsing habits. In addition to all this, spyware inevitably affects the performance of a phone or computer (Stafford, T. F., & Urbaczewski, A., 2004).

Adware, pornography, and dangerous software include legitimately developed programs that can, in some cases, be used to pose specific threats to computer and phone users (including acting as spyware). Although these programs may have been developed and distributed by legitimate companies, they may include functions that some malware creators use for malicious or illegal purposes (Boldt, M., Carlsson, B., & Jacobsson, A., 2004).

Spyware is prevented when installing any program on a phone or computer. It is necessary to ensure that you carefully read all disclosure information, including the license agreement and privacy statement. Sometimes the unwanted software included in the installation of a certain program may already be documented, and it may appear at the end of the license agreement or privacy statement (Herley, C. E., et al, 2015).

## 6- keylogger

Simply put, a keylogger is a tool designed to capture all keystrokes of a computer either through a program or a device / tool. This keyboard recording activity is also referred to as keylogging or keystroke logging. Although keylogger is not illegal, its use is often linked to malicious processes (Davarpanah Jazi, et al, 2014).

A keylogger is to record every keystroke from the target computer and it's not necessarily a bad thing. Unfortunately, the most common use of a keylogger is related to malicious activities.

Keyboard monitoring software is widely used by cybercriminals as a way to steal sensitive information from victims such as credit card numbers, passwords, and personal emails, Bank credits, driver's license numbers, etc. (Olzak, T., 2008).

There are two main types of keyloggers, one version of a hardware (hardware) version and a copy of a software (a program). When it comes to the comparison between hardware and software, it is important to understand the differences between the two types. Although the most popular type is software, one must still understand how a keylogger works as well (Creutzburg, R., 2017).

The easiest way to detect software keyloggers is to check what is running on the system processes. If something seems strange, you should search the Internet and try to find out if it is a legitimate program or a known keylogger. Moreover, checking and checking the traffic leaving your computer is a good idea as well (Dadkhah, M., & Jazi, M. D., 2014).

Getting rid of software keyloggers is not easy but it can be done. You must first try to install an anti-malware program Keyloggers on your device and check if they can be removed. If your computer is still running erratically and you suspect that the anti-keylogger software was not able to solve the problem, you may have to reinstall the operating system completely (Tuscano, A., & Koshy, T. S., 2020).

## Malware detection systems:

### IObit Malware Fighter Free

Free Malware Fighter 6.2 is part of IObit's protection and performance improvement program, which includes Driver Booster, Advanced Systemcare, Smart Defrag, Password Manager, etc.

This program is a protection package that aims to protect Internet browsing from the latest harmful threats such as ransomware and adware. It detects all types of malware, there are different types of scan (basic, complete and direct) and it is very easy.

One of its advantages is that it provides a wide database of threats, it is updated regularly, the ability to detect types of malware for different scenarios, it notifies users about any new ransomware program in alerts.

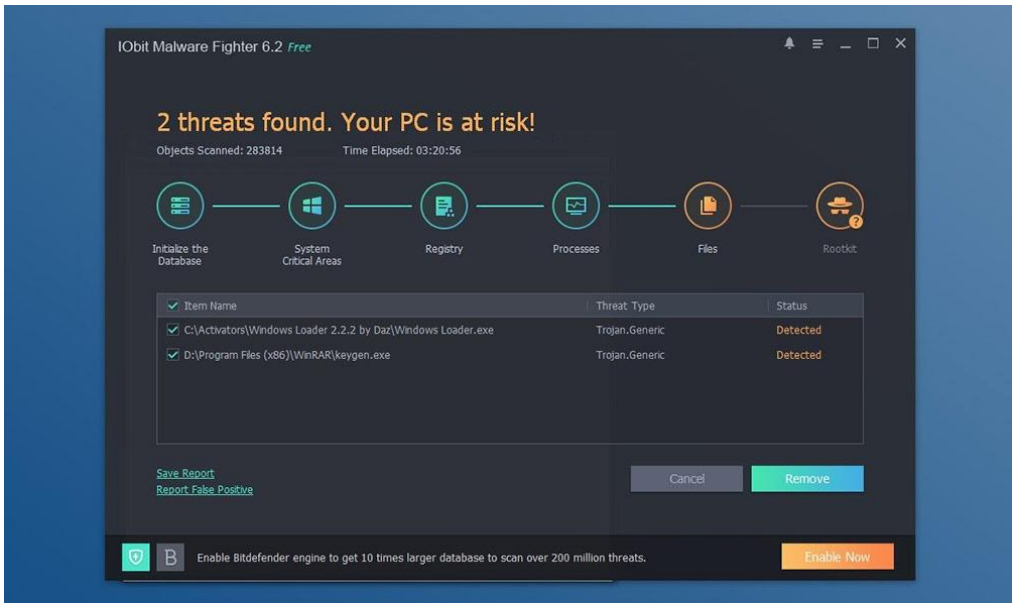


*Figure 1: IObit Malware Fighter Free*

## iolo System Mechanic Ultimate Defense

Mechanical Maximum Defense System is a new program from IOLO that offers a modern and comprehensive solution. It is implemented by 6 layers of protection (modules), the main component being the anti-malware scanner in real time. Certified VB-100 technology finds and stops harmful files in early stages by applying behavioral analysis. To speed up scanning and detection, the mechanical system is characterized by the presence of a database that contains the most important and comprehensive virus and harmful files, which at the same time excludes reliable files from scanning to save computer resources and time. Byepass password manager and automatic privacy cleaner are integrated as part of a secure network system. Characterized by providing perfect results in testing, the built-in PC Optimizer is the ability to recover deleted files.

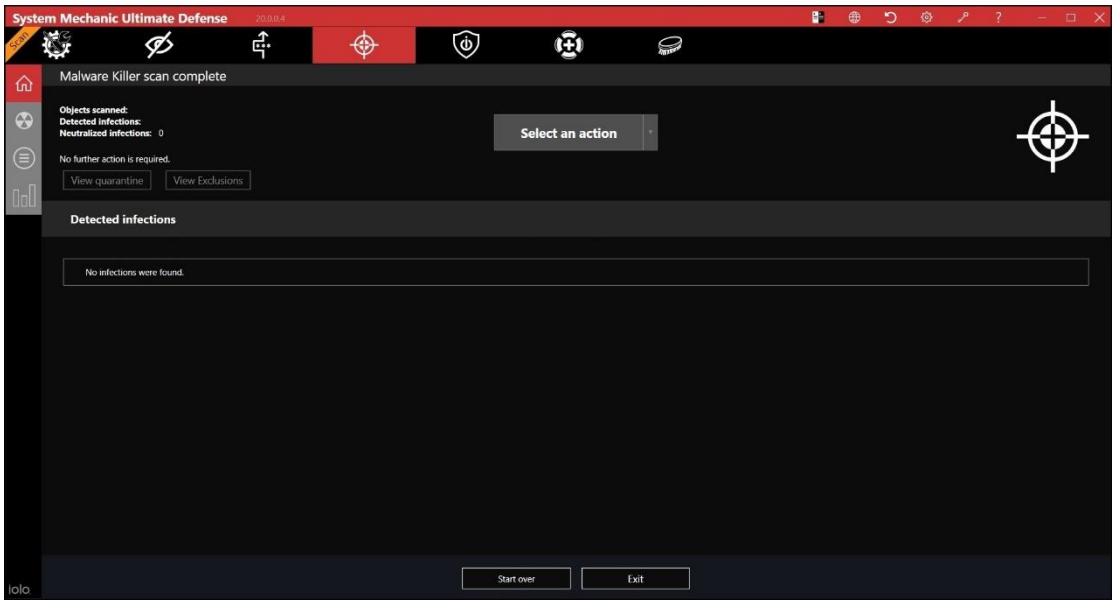


*Figure 2: iolo System Mechanic Ultimate Defense*

## Malwarebytes

It was developed to provide multi-level protection for personal computers by cleaning and saving all forms of malware currently known. Also, the free version of Malwarebytes gets rid of spyware easily by identifying and removing any suspicious files. Malwarebytes is an anti-malware program that detects and removes infected computer files. the free version is actually a 14-day trial.

It is characterized by the ability to detects and removes spyware, botnets, Trojan horses, and other viruses, very easy to use and has clear instructions that can be easily followed, and enhances instant protection against viruses when used with anti-virus software.

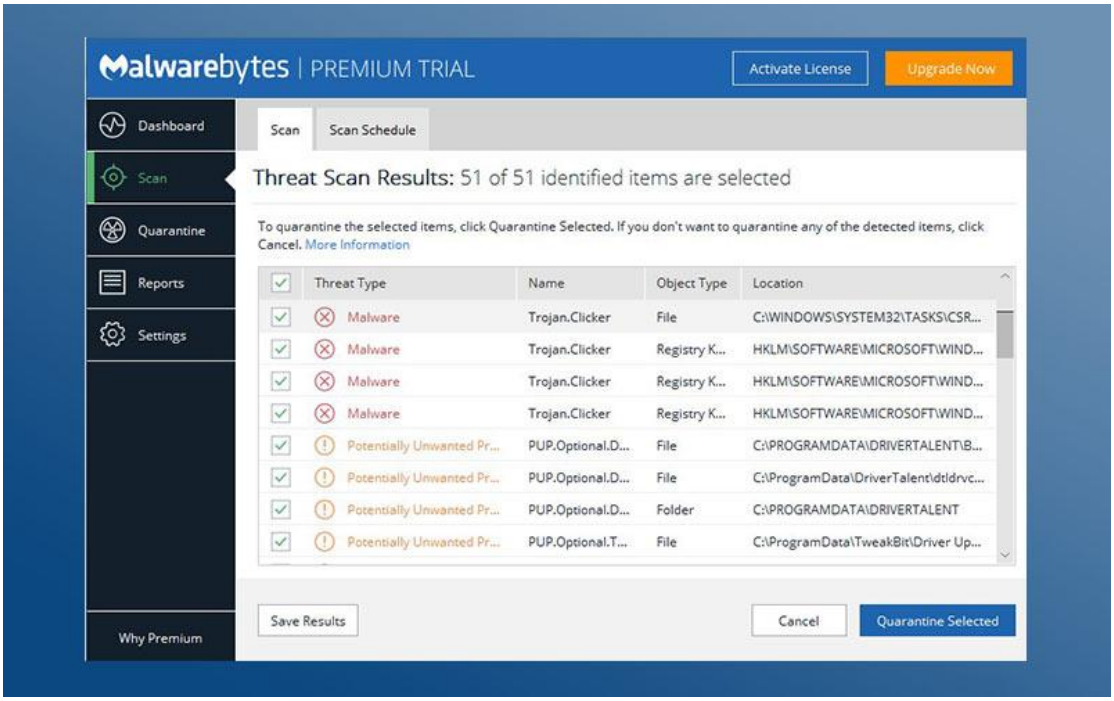


*Figure 3: Malwarebytes*

## Kaspersky Internet Security

The new antivirus product from Kaspersky Lab now comes equipped with a malware defense module, and consumes fewer system resources thanks to the rebuilt algorithms. It enables you to manage devices in your My Kaspersky account, which also provides access to a password manager and parental control options.

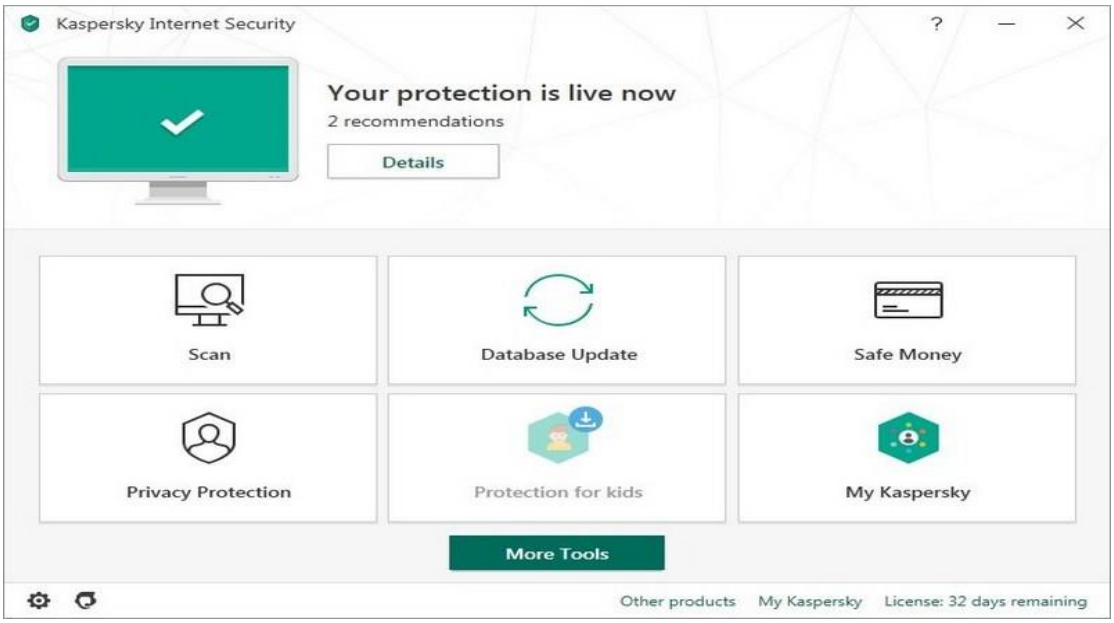


*Figure 4:Kaspersky Internet Security*

## Impact of malware detection for mobile

Usually malware and malicious codes hide in fake versions of popular applications, the user must check whether the application in question is developed by the same company, and here the evaluations of other users can be used, and the user must be careful and careful when dealing with applications that promote themselves By making paid content available for free, or applications, that can add new functions to popular applications, which the original applications do not provide.

Consequently, many users may resort to dealing with a special system to detect malware for mobile phones, due to the large threat situations and thus justify the abundance of offers from malware detection programs, as new attacks targeting the phone are always detected, in addition to the constantly increasing risk of malware Such as data encryption and ransomware viruses, so there is no substitute for protecting the phone well, as it works to provide safe protection on an ongoing basis. Knowing about malware is the first step in protecting your phone from attacks

Most malware can be avoided by applying some common sense when downloading and opening files from various sources. However, for complete security.

## Conclusion:

Dealing with malware, known as malware, is a reality we all face when online. Nobody wants to open their email to discover that they have just sent an infected file to all of their friends, or their data has been erased due to a virus. Although most people fear viruses, they are also surprisingly unaware of what malware is and how it does its malicious work.

Consequently, many users may resort to dealing with a special system to detect malware for mobile phones, due to the large threat situations and thus justify the abundance of offers from malware detection programs, as new attacks targeting the phone are always detected, in addition to the constantly increasing risk of malware Such as data encryption and ransomware viruses, so there is no substitute for protecting the phone well, as it works to provide safe protection on an ongoing basis.

Thus, it may be required to download and deal with special programs to detect malicious software for mobile phones, thus helping users to detect and deal with these programs.

## References:

[1] Aycock, J. (2006). Computer viruses and malware (Vol. 22). Springer Science & Business Media.

[2] Bayer, U., Habibi, I., Balzarotti, D., Kirda, E., & Kruegel, C. (2009, April). A View on Current Malware Behaviors. In LEET.

[3] Blake, H. (2008). Innovation in practice: mobile phone technology in patient care. British journal of community nursing, 13(4), 160-165.

[4] Boldt, M., Carlsson, B., & Jacobsson, A. (2004). Exploring spyware effects. In Nordsec 2004.

[5] Bose, A., & Shin, K. G. (2006, September). On mobile viruses exploiting messaging and bluetooth services. In 2006 Securecomm and Workshops (pp. 1-10). IEEE.

[6] Bryce, T. (2006). The Trojans & Their Neighbours. Routledge. https://books.google.com/books?hl=en&lr=&id=dWXbuQ7OiJQC&oi=fnd&pg=PP1&dq=Trojans+Horse+&ots=UNmu6DLMiF&sig=9DAFhpwAMokZPewJMI_wnG6-_Fs

[7] Chen, Z., Gao, L., & Kwiat, K. (2003, March). Modeling the spread of active worms. In IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428) (Vol. 3, pp. 1890-1900). IEEE.

[8] Creutzburg, R. (2017). The strange world of keyloggers-an overview, Part I. Electronic Imaging, 2017(6), 139-148.

[9] Dadkhah, M., & Jazi, M. D. (2014). A novel approach to deal with keyloggers. Oriental Journal of Computer Science & Technology, 7(1), 25-28.

[10] Davarpanah Jazi, M., Ciobotaru, A. M., & Barati, E. (2014). An Introduction to Undetectable Keyloggers with Experimental Testing. International Journal of Computer Communications and Networks (IJCCN), 4(3), 1-5.

[11] Dunham, K. (2008). Mobile malware attacks and defense. Syngress.

[12] Filiol, E. (2010). Viruses and malware. In Handbook of Information and Communication Security (pp. 747-769). Springer, Berlin, Heidelberg.

[13] Fuentes, D., Álvarez, J. A., Ortega, J. A., Gonzalez-Abril, L., & Velasco, F. (2010). Trojan horses in mobile devices. Computer Science and Information Systems, 7(4), 813-822.

[14] Funk, J. L. (2004). The product life cycle theory and product line management: the case of mobile phones. IEEE Transactions on Engineering Management, 51(2), 142-152.

[15] Geer, D. (2005). Malicious bots threaten network security. Computer, 38(1), 18-20.using fictitious play. International Journal of Automation and Computing, 9(2), 122-134.

[16] Grégio, A. R. A., Afonso, V. M., Filho, D. S. F., Geus, P. L. D., & Jino, M. (2015). Toward a taxonomy of malware behaviors. The Computer Journal, 58(10), 2758-2777.

[17] Herley, C. E., Keogh, B. W., Hulett, A. M., Marinescu, A. M., Williams, J. S., & Nurilov, S. (2015). U.S. Patent No. 9,021,590. Washington, DC: U.S. Patent and Trademark Office.

[18] http://www.tkqlhce.com/click-8815956-13801426&AFFSRC=h2_ar

[19] https://secure2.iolo.com/affiliate.php?ACCOUNT=IOLO&AFFILIATE=112984&PATH=http%3A%2F%2Fwww.iolo.com%3FAFFILIATE%3D112984

[20] https://thinkmobiles.com/products/35563/

[21] https://www.dpbolvw.net/click-8815956-11633246?sid=h2_ar

[22] Hypponen, M. (2006). Malware goes mobile. Scientific American, 295(5), 70-77.

[23] Hypponen, M. (2006). Malware goes mobile. Scientific American, 295(5), 70-77.

[24] Kondakci, S. (2008). Epidemic state analysis of computers under malware attacks. Simulation Modelling Practice and Theory, 16(5), 571-584.

[25] Lawton, G. (2008). Is it finally time to worry about mobile malware?. Computer, 41(5), 12-14.

[26] Moberg, Å., Borggren, C., Ambell, C., Finnveden, G., Guldbrandsson, F., Bondesson, A., ... & Bergmark, P. (2014). Simplifying a life cycle assessment of a mobile phone. The International Journal of Life Cycle Assessment, 19(5), 979-993.

[27] Olzak, T. (2008). Keystroke logging (keylogging). Adventures in Security, April.

[28] Patel, U. K., Patel, P., Hexmoor, H., & Carver, N. (2012). Improving behavior of computer game bots

[29] Peng, S., Yu, S., & Yang, A. (2013). Smartphone malware and its propagation modeling: A survey. IEEE Communications Surveys & Tutorials, 16(2), 925-941.

[30] Pratama, A., & Rafrastara, F. A. (2012). Computer worm classification. International Journal of Computer Science and Information Security, 10(4), 21.

[31] Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. Future Generation Computer Systems, 97, 887-909.

[32] Russell Ware (24-2-2018), "? What is a Cell Phone" ،lifewire, Retrieved 15\1\2021. Edited. https://www.lifewire.com/what-is-a-cell-phone-577492

[33] Stafford, T. F., & Urbaczewski, A. (2004). Spyware: The ghost in the machine. The Communications of the Association for Information Systems, 14(1), 49.

[34] Toutonji, O., & Yoo, S. M. (2009). An approach against a computer worm attack. International Journal of Communication Networks and Information Security, 1(2), 47.

[35] Tuscano, A., & Koshy, T. S. (2020). Types of Keyloggers Technologies–Survey. In ICCCE 2020 (pp. 11-22). Springer, Singapore.

[36] Weaver, N., Paxson, V., Staniford, S., & Cunningham, R. (2003, October). A taxonomy of computer worms. In Proceedings of the 2003 ACM workshop on Rapid malcode (pp. 11-18).

[37] Wessel, M., De Souza, B. M., Steinmacher, I., Wiese, I. S., Polato, I., Chaves, A. P., & Gerosa, M. A. (2018). The power of bots: Characterizing and

understanding bots in oss projects. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 1-19.

[38] Zhang, X., & Tehranipoor, M. (2011, June). Case study: Detecting hardware Trojans in third-party digital IP cores. In 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (pp. 67-70). IEEE.

[39] Zhenfang, Z. H. U. (2015). Study on Computer Trojan Horse Virus and Its Prevention. International Journal of Engineering and Applied Sciences, 2(8).

[40] Zyba, G., Voelker, G. M., Liljenstam, M., Méhes, A., & Johansson, P. (2009, April). Defending mobile phones from proximity malware. In IEEE INFOCOM 2009 (pp. 1503-1511). IEEE.