ISSN 2347 - 3983
Volume 8. No. 7, July 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter07872020.pdf
https://doi.org/10.30534/ijeter/2020/07872020

# A Method for Identifying and Countering HID Attacks - Virus Detection in BMP Images

**Grynov Rostyslav[1],Vitalii Martovytskyi[1],Oleksandr Sievierinov[1],Vladislav Sukhoteplyj[2], Olha Soloviova[3], Yelizaveta Kortyak[1]**
[1]Kharkiv National University of Radio Electronics, Ukraine, Kharkiv, 61166,Naukiave., 14, dec@nure.ua
[2]Ivan KozhedubKharkiv National Air Force University,Ukraine, Kharkiv,61023 Sumska av. 77/79, vladislav181168@gmail.com
[3]Ivan KozhedubKharkiv National Air Force University,Ukraine, Kharkiv,61023 Sumska av. 77/79, olga01@ukr.net

## ABSTRACT

The aim of the article - develop a method for protecting modern systems from attacks using BMP image files and HID attacks. This article describes the features of BMP format images. The method of injecting computer viruses in BMP image and attacks in order to overcome the means of protection. The article suggests methods for detecting viruses in BMP image files and counteracting HID attacks. Developed programs demonstrate the effectiveness of protection against the considered attacks

**Key words :**BMP image file; computer virus; shell code; overcoming protection systems; virus hiding; antivirus; IDS; IPS; vulnerability; exploit; HID attack; protection methods.

## 1. INTRODUCTION

We trust confidential information to a variety of technical equipment (telephones, computers, smart watches). Over time and the development of technology, their number is continuously growing. Attackers create new techniques for hiding and spreading computer viruses [1-4]. Therefore, the task of searching and countering computer viruses is relevant not only for ordinary users but also for large firms and companies. Recently, the possibilities of steganography are widely used to hide computer viruses [5, 6].

That is why, to protect user data, various means of information protection have been developed and are still being created. For example, antivirus software, intrusion detection systems (IDS), intrusion prevention systems (IPS) and firewalls [7]. However, even these tools may not be enough to protect data.

## 2. METHOD OF OVERCOMING PROTECTION USING VULNERABILITIES IN BMP IMAGE FILE FORMAT

Attackers add various new functions to viruses and develop new methods for hiding malicious code in order to overcome protection tools [8]. Attackers can use steganography to inject virus software into the image, to bypass anti-virus tools, IDS / IPS, and sandboxes. Before a virus is launched on an employee's computer, many devices will analyze it.

Most file analysis methods include using virus signatures and analyzing behavior in the sandbox, namely:

- verification of running processes;
- checking the current domain;
- checking uptime;
- check disk size;
- check the amount of memory.

Security systems are designed in such a way that most sandboxes will only analyze executable files, DLLs, Word documents, Java applets [9]. Most of the protections simply do not pay attention to images or another secure file type. Since they believe that there is no reason to spend the processor cycle on image analysis [10]. Checking all types of files for the presence of a virus can lead to serious system load, slow down its operation, and reduce the channel bandwidth, which can lead to serious consequences. This situation is especially critical in our time when you need to quickly process large amounts of data.

For example, an attacker can inject a virus into a BMP image so that the user does not notice anything suspicious. He will not see any strange points in the image. This is due to the features of the BMP image format. Writing a virus into an image will distort the color information of the pixels, as the data will be replaced. However, BMP images have special fields in the header, which are responsible for the displayed number of pixels horizontally and vertically. By changing the value of these fields, we can achieve a result when distorted pixels are not displayed, but the information in the file itself remains[11]. Due to the artificial reduction of the image height by several pixels in the header, distorted pixels can be hidden, but a person will not notice it [10].

The injection is possible because bytes that indicate the type of file with which the file begins, BM in ASCII, in hexadecimal is 42 4D, when converted to assembler instructions, they do not lead to an execution error, and the subsequent 8 bytes of the header does not affect image interpretation [10]. These 8 bytes consist of two reserved

fields that take the value 0 and a field that indicates the file size in bytes. Their modification does not affect the correctness of displaying the file size and the image as a whole in various operating systems and programs for viewing graphic images. These 8 bytes can be filled with any assembler instructions, for example, you can write a jmp instruction in them, which will indicate a virus that will be stored at the end of the image. An attacker could use a set of PowerShell commands to execute code stored in an image.

This attack is made even more dangerous by the fact that it can be combined with HID attacks [12]. For example, an attacker can program a microcontroller so that when it connects, it opens a command prompt, enters, and executes a PowerShell command that will load the image and launch the virus. Such a device can be disguised as a flash drive, keyboard, or other peripheral equipment [13].

The main danger of such images with viruses is that non-standard methods must be used to identify the threat. You can try to change the settings of the protection tools so that they check all types of files, but this will significantly slow down and also can completely paralyze the work of the entire information and communication system. Also, the use of such attacks can greatly complicate the analysis of an information security incident in an organization.

Firstly, this is due to the fact that security systems may not respond to the virus and it will be very difficult to detect the fact of penetration. And by the time the fact of compromising the system is revealed, a lot of time may pass and serious damage will be caused to the system.

Secondly, if the fact of penetration is established, it will be almost impossible to find out how this happened. Because, first of all, the employees of the security department will find out which executables, DLLs, Microsoft Office documents, PDF files have got into the system and have been used recently. And even the approximate date of penetration is not known, the amount of information that needs to be processed will increase significantly. In this case, none of the workers will examine the image files.

Since the image cannot be run as an executable file, both the protection tools and technical specialists can be frivolous about its contents and neglect this threat.

However, such a file can be a serious danger. Intrusion prevention and detection systems must be configured in a manner. Investigations into information security incidents need to be carried out more thoroughly. In addition, it is necessary to develop new systems and methods of protection against the considered attacks.

## 3. HID-ATTACKS

HID attacks have been known for a long time, but their use is quite rare for the modern world. Malicious HID devices can be of various shapes and disguised as different equipment, but they all perform the same tasks. Most often, they look like ordinary flash drives, but in fact HID devices pretend to be a keyboard in the system. The main idea of this attack vector is that the keyboard, like other HID devices, is trusted for the system and security tools, unlike executable files that are checked by security tools for the presence of computer viruses. When you connect a similar malicious HID device, it begins to perform programmed actions. In our case, a similar device, when connected, can open PowerShell and execute commands that download images and execute the virus that is in it. HID devices are considered by the system and anti-virus protection tools as a simple interface between the user and the system. Therefore, for all protection systems, this is the usual user input of commands from the keyboard, which does not carry any danger, and the device is just a simple keyboard. Using malicious HID devices, an attacker can compromise a computer system without having to interact directly with it.

## 4. METHODS FOR DETECTING VIRUSES IN BMP IMAGE FILES

First of all, in order to counteract the attack described in work, it is necessary to develop new means of protection and methods for detecting viruses. Namely:

- anti-virus protection tools must scan image files for viruses, including using "masks";
- scan BMP image files for any data in reserved header fields other than zeros. If these fields have non-zero values, this may mean that a virus has been injected into the file;
- if the "Size" field in the file header does not match the file size in bytes, this may also indicate a hidden malicious code;
- based on the amount of pixel data, you can get information about the actual size of the image in pixels, if it does not match the width and height specified in the header, this may indicate the presence of a built-in virus;
- it is also possible to use programs that detect anomalies in the image to detect malicious code. So, in the presence of a large number of distorted points, it can be argued that there is a virus in the image.

A significant drawback of this approach is the need for a detailed analysis of files and the use of computer resources. With a heavy load of ITS, this can lead to serious disability and denial of service. Also, to prevent such attacks, you must:
- clearly define the list of available Internet resources for users. This will make it impossible to place the infected image on web-resources to which attackers have access;
- filter and control organization traffic. If possible, prevent employees from downloading executable files, scripts, dynamic link libraries (DLLs). Also, download documents from unknown sources created in Microsoft Office and the like, as well as BMP image files.

During the study, a program was developed in Python that checks the reserved BMP image fields, the SIZE field also determines the real number of pixels and compares this value with the number of horizontal and vertical pixels indicated in the image header.

When checking the original image, no anomalies were found (Figure 1).

When checking the infected image, anomalies were detected by key signs (Figure 2).

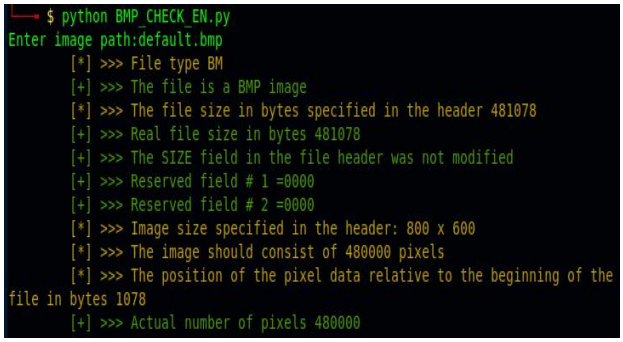


**Figure 1:**Checking the original image

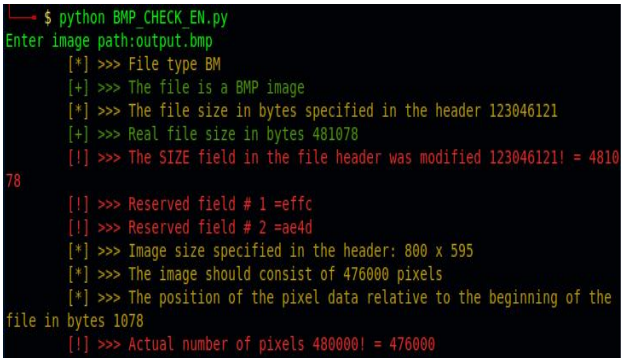


**Figure 2:**Checking an infected image

## 5. METHODS FOR DETECTING AND COUNTERACTING HID-ATTACKS

To identify and counter HID attacks, you must:

- check purchased equipment and equipment after repair for the presence of embedded devices. Conduct periodic inspection of existing equipment;

- restrict access to equipment of unauthorized persons and workers who do not interact with it;
- request login and password for authentication when starting PowerShell and CMD, not only for the administrator but also for any user;

- a ban on the installation of removable devices can be implemented using group security policy, both for the local machine and for workstations in the domain. However, "Plug'n'play" will not be available;

- use of the "white list" - a list of trusted devices. However, it should be noted that devices are identified by the system using a combination of Vendor ID and Product ID, which can be programmed by an attacker and fully correspond to those already registered in the system. Thus, even white list blocking is not an absolute defense;

- One of the most effective means of protection against HID attacks is the use of heuristic analysis methods for detection and blocking, for example, based on the analysis of changes in input speed.

In the course of the study, a Python program was also developed to identify and counter HID attacks based on an analysis of the text input speed and its changes. If the input speed has increased significantly and it is much higher than the person's possible input speed, the program will detect an attack. The program has 4 modes:

- when an attack is detected, it will simply be registered in the journal, without opposition;

- when an attack is detected, a few keystrokes will be interrupted (this is enough to interrupt any attack, it looks like the attacker made a mistake.) The attack will also be logged;

- when an attack is detected, keyboard input will be temporarily disabled. After the attack is completed, keyboard input will again be allowed. The attack will be recorded in the journal;

- when an attack is detected, the protection program blocks all subsequent keystrokes until the correct password is entered. (You can set the password in the .conf file). The attack will also be logged.

The program does not have a graphical interface. After starting, the program functions as a background process. An attack on a computer running the Windows 10 operating system is shown in Figure 3. It is worth noting that all versions of the operating systems of the Windows and Linux family are vulnerable to this attack. MacOS is also vulnerable to these attacks.


**Figure 3:**Successful attack on an unprotected system.

After starting the program, HID attacks were detected and neutralized.

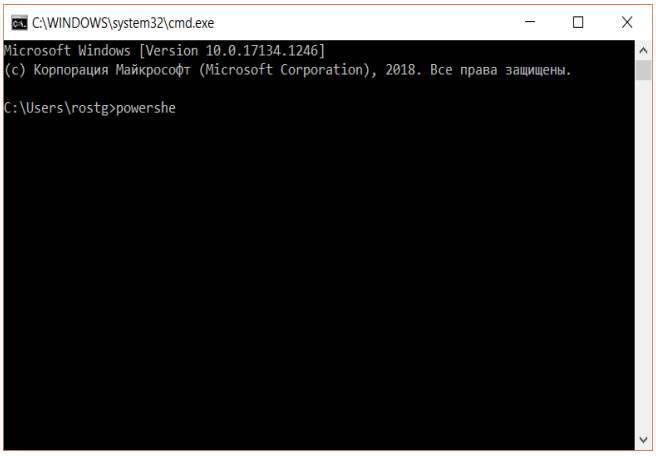


**Figure 4:**Identified and neutralized attack using the developed program

## 6. CONCLUSION

Using the developed attack method, we successfully overcame defense systems and gained remote access. Classic defense systems could not identify and prevent this attack. Which indicates its danger to modern protection systems. During the tests, the virus in the image was not detected by any means of protection, in addition, the tests were carried out with a variety of antivirus solutions. The HID attack was also not detected due to the specifics and characteristics of this attack.

In the course of the research, a method was developed and demonstrated to detect the hidden virus in BMP images. A program has also been created to detect and counter HID attacks. After analyzing the results, it can be argued that this method of detecting a hidden virus allows us to detect hidden malicious code in BMP images successfully. Also, the program for protecting against HID attacks successfully detected and neutralized the HID attack. According to the test results, it can be argued that the developed methods for detecting hidden virus code in a BMP image and countering HID attacks are more effective in countering these attacks than modern protection tools. The results of this work can be used in the development of anti-virus protection tools and comprehensive ITS protection tools and for their modernization to prevent such attacks.

It should be remembered that even ordinary files with a simple structure without script support can pose a serious threat. Therefore, it is necessary to develop new, more effective remedies. The main danger of such images with viruses is that non-standard methods must be used to identify the threat. You can change the settings of the protection tools so that they check all types of files, but this will significantly slow down or even completely paralyze the work of the entire information and communication system.

The best methods for detecting viruses hidden in BMP images are based on:

- scan BMP image files for any data in reserved header fields other than zeros. If these fields have non-zero values, this may mean that a virus has been injected into the file;

- if the "Size" field in the file header does not match the file size in bytes, this may also indicate a hidden malicious code;

- based on the amount of pixel data, you can get information about the actual size of the image in pixels, if it does not match the width and height specified in the header, this may indicate the presence of a built-in virus;

- it is also possible to use programs that detect anomalies in the image to detect malicious code. So, in the presence of a large number of distorted points, it can be argued that there is a virus in the image.

One of the most effective means of protection against HID attacks is the use of heuristic analysis methods for detection and blocking, for example, based on the analysis of changes in input speed.

## REFERENCES


1. I. Ruban, V. Martovytskyi and N. Lukova-Chuiko, **Designing a monitoring model for cluster super-computer**, *Eastern-European Journal of Enterprise Technologies*, vol. 6, no. 84, pp. 32-37, 2016 https://doi.org/10.15587/1729-4061.2016.85433
2. O. Barabash, V. Sobchuk, N. Lukova-Chuiko and A. Musienko. **Application of Petri Networks for Support of Functional Stability of Information Systems**. *2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC)*. 08-12 October, Igor Sikorsky Kyiv Polytechnic Institute, 2018. Kyiv, Ukraine. P. 36 – 39.
3. Acar, Abbas, et al. **"An analysis of malware trends in enterprise networks."***International Conference on Information Security*. Springer, Cham, 2019. https://doi.org/10.1007/978-3-030-30215-3_18
4. Liashenko, O., Barkovska, O., Al-Atroshi, C., Datsok, O., Liashenko, S. **Model of the work of the neurocontroller to control fuzzy data from the sensors of the climate control subsystem "smart house",** *International Journal of Advanced Trends in Computer Science and Engineering*, 8(1), Pp. 70-74
5. Iliev, Anton, et al.**"Some models in the theory of computer viruses propagation."** *LAP LAMBERT* Academic Publishing (2019.
6. Pare. **Virus spread over networks: Modeling, analysis, and control** *:Ph.D. Electrical & Computer Eng* / Pare. – Uni-versity of Illinois at Urbana-Champaign, 2018.
7. Jingwei LEI. **Virus program detection method, terminal, and computer readable storage medium** / *Jingwei LEI*. – United States, 2018. – 19 с.
8. Wen-Kwang Tsao. **Detecting malicious code in sections of computer files,** Wen-KwangTsao, Pinghuan Wu, Zipan Bai. – United States, 2018. – 15 с.
9. LubomirSikora. **Swarm Virus, Evolution, Behavior and Networking** / LubomirSikora, Ivan Zelinka. – Berlin, 2017.
10. Carey Parker. **Computer Security** / Carey Parker. – North CarolinaUSA, 2018.
11. Ruban, I., Bolohova, N., Martovytskyi, V., Lukova-Chuiko, N., Lebediev, V. / **Method of sustainable detection of augmented reality markers by changing deconvolution,** *International Journal of Advanced Trends in Computer Science and Engineering*, Volume 9 No.2, pp. 1113-1120, 2016 https://doi.org/10.30534/ijatcse/2020/33922020
12. Zhao, Songyin, andXuAnWang. **"A SurveyofMalicious HID Devices."** *International Conference on Broadband and Wireless Computing, Communication and Applications*. Springer, Cham, 2019.
13. Karystinos, Evangelos, Antonios Andreatos, and Christos Douligeris. **"Spyduino: Arduino as a HID Exploiting the BadUSB Vulnerability.***"2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 2019. https://doi.org/10.1109/DCOSS.2019.00066