Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.123 – 133

Create a Software Firewall to Protect Web Applications, Websites, Databases and What is so Tempting to Cyber Criminals

ABDULLAH FARHAN

AGRICULTURE COLLEGE, DIYALA UNIVERSITY, IRAQ

U_BOD@sport.uodiyala.edu.iq

Abstract

As the Internet has evolved over the years, it has become an integral part of virtually every aspect in the business process cycle. In the early days of the Web a company's online presence consisted of a static website that promoted products and provided visitors with company information. The emergence of certain technologies like AJAX, PHP, and Document Object Models gave businesses the ability to move from placing nothing short of a company brochure on the Web to deploy dynamic, feature-rich applications that drive sales through e-commerce; provide online services to their employees; establish open ended communication between themselves and their customers; and allow for collaboration among employees, partners, suppliers, and clients. In addition to providing employees and customers with a more dynamic experience, Web applications have become a way for businesses to save money. By turning to Software as a Service and cloud based solutions, organizations have found that they are able to trim their budgets by:

• Spending less on resources such as servers and networking infrastructure

• Reducing power consumption and related costs

• Avoiding capital expenditures associated with IT

• Using technology that is flexible and scalable

© 2017, IJCSMC All Rights Reserved

Of course, as the usefulness and complexity of the Internet grew through increased use of web applications, the security risks involved also grew proportionately. To combat the threats that these applications face, many organizations look towards traditional network security solutions. Thinking that deploying a network firewall, intrusion detection system, or intrusion prevention system works to protect the network perimeter from attack at the application layer (OSI Layer-7) can be a huge mistake. The traditional approach to network security aims to protect resources such as servers, workstations, printers, internal databases, and other network resources. The tools used to secure these resources work by preventing access to certain ports or services by creating allow or deny rules to network packets. Blocking access to port scans, worms, viruses, and other attacks aimed at networking protocols works to prevent intrusion over OSI Layer-3, but does nothing to prevent the sophisticated attacks that take place at the application layer because their simple approach does not work in an environment where each application differs from another. Web application security relies on the ability to inspect HTTP packets to handle threats at Layer-7 of the OSI model. Attackers are all too familiar with the fact that traditional perimeter security methods do not stop attacks against Web applications that are, by nature, designed to allow visitors to access data that drives the Website. By exploiting simple vulnerabilities in Web applications, an attacker can pass through perimeter security undetected accessing data and even the network your traditional firewall and IDS systems are in place to protect.

Introduction

Bitdefender is a Romanian Internet security software company, represented through subsidiaries and partners in over 100 countries.[1] The company has been developing online protection since 2001. In September 2014, the company claimed to have its technologies installed in around 500 million home and corporate devices across the globe.[2] Bitdefender replaced SOFTWIN's earlier AVX[3] (AntiVirus eXpert) product range. Between 1996 and 2001 AVX became a product available worldwide that offered intelligent updating without user intervention and integrated an internal browser which scanned and monitored all downloaded files. AVX pioneered behavior-based application blocking technology[4] and was also the first antivirus product to include personal firewall features. With the sixth generation of AVX, the product became the first antivirus package to include an application firewall as well as behavior-based blocking. The Bitdefender group spun off from SOFTWIN in 2007. Data leakage protection: prevent sensitive information disclosure using built-in and extensible outgoing traffic inspection rules. Mitigate proliferation of credit card, personal information, application error messages into the wrong hands. Upload inspection: upload content inspection enforces file extension and MIME-type filtering. Prevent web shells, backdoors and rootkits from being uploaded via Web content management systems. Scan contents of uploaded files to ensure malicious payloads are not smuggled in posing as benign pictures and content.

© 2017, IJCSMC All Rights Reserved

Definition risks of web applications

To help it professionals better understand the security risks that surround web applications, a community of concerned individuals created the open web application security project or OWASP for short. In addition to a collection of open source tools, training and projects, OWASP publishes a list of the top ten risks to web application security. Among the most prevalent threats to web applications are:

Injection attacks (1)

Cross-site scripting (2)

Security misconfiguration (6)

Failure to restrict url access (7)

Injection attacks are the result of a Web application sending untrusted data to the server. The most common attack occurs from malicious code being inserted into a string that is passed along to a SQL Server for execution. This attack, known as SQL Injection, allows the attacker access to data which can be stolen or manipulated. Other types of injection attacks include Code Injection and Carriage Return/Line Fee (CRLF) Injection .Cross-Site Scripting, or XSS, is the most prevalent security flaw that Web applications are vulnerable to In an XSS attack, the attacker is able to insert malicious code into a Website. When this code is executed in a visitor's browser it can manipulate the browser to do whatever it wants. Typical attacks include installing malware, jacking the user's session, or redirecting a user to another site. Security Misconfiguration is the result of poor administration of the Web server or application server and often leads to path traversal vulnerabilities. Allowing unauthorized or unprotected access to files directories or accounts can lead to an attacker completely promising a system that is vulnerable. Failure to protect URL access is another flaw that allows attackers to exploit the path traversal vulnerability. Only in this case, the attacker simply amends the URL to see if he is granted access to a private page or directory within the Website.

Bitdefender software firewall

Bitdefender is a Romanian Internet security software company, represented through subsidiaries and partners in over 100 countries.[1] The company has been developing online protection since 2001. In September 2014, the company claimed to have its technologies installed in around 500 million home and corporate devices across the globe.[2] The Bitdefender products include anti-virus and anti-spyware capabilities against Internet security threats such as viruses, Trojans, rootkits, rogues, "aggressive adware," spam and others, and that their applications include web protection, cloud antispam, firewall, a vulnerability scanner, parental controls, file encryption, device anti-theft and backup for corporate and home users. In 2016, the company claimed that its products now include profiles for performance optimization, a secure browser

© 2017, IJCSMC All Rights Reserved

for online transactions, and a virtual wallet option to save passwords. Bitdefender replaced SOFTWIN's earlier AVX[3] (AntiVirus eXpert) product range. Between 1996 and 2001 AVX became a product available worldwide that offered intelligent updating without user intervention and integrated an internal browser which scanned and monitored all downloaded files. AVX pioneered behavior-based application blocking technology[4] and was also the first antivirus product to include personal firewall features. With the sixth generation of AVX, the product became the first antivirus package to include an application firewall as well as behavior-based blocking. The Bitdefender group spun off from SOFTWIN in 2007. Bitdefender makes antivirus products for home users as well as businesses. Home editions support Microsoft Windows, Mac OS X, Android and iOS. Bitdefender competes in the antivirus industry against Avira, BullGuard, FRISK, Kaspersky, McAfee, Panda Security, Sophos, Symantec and Trend Micro among others. Bitdefender Total Security Multi-Device is a security suite for Windows, Mac and Android devices that is claimed to protect the devices through machine-learning technologies to improve malware detection and enhance proactive security. The company claims that the technology is based on processing the newest malware information available to predict and block future outbreaks as fast as possible. Bitdefender Family Pack is designed for families, offering privacy protection through parental control, device anti-theft, safer online banking and shopping, password management tools and other features. For Windows-based computers, the products Bitdefender Total Security, Bitdefender Internet Security, and Bitdefender Antivirus Plus are designed to protect end-users through anti-phishing and antispam modules, firewall and anti-virus protection, plus other features. For Android users, the company offers a cloud-based security solution with anti-malware and anti-theft capabilities called Bitdefender Mobile Security. Bitdefender BOX is the only hardware device from Bitdefender's portfolio designed to protect smart home networks and inter-connected Internet of Things devices. Bitdefender GravityZone is an enterprise security solution for medium to very large organizations. It is available in three commercial offers: GravityZone Business Security, GravityZone Advanced Business Security and GravityZone Enterprise Security, which include security for endpoints, virtualized environments, Exchange servers and mobile terminals. Bitdefender endpoint protection was included in the Gartner Magic Quadrant,[5] a focused analysis on market insights by reputable American advisory firm Gartner.

© 2017, IJCSMC All Rights Reserved

Home/Home Office[6]	Business Solutions[7]	Tech Assist[8]	Free Tools[9]
Bitdefender BOX	Bitdefender GravityZone Enterprise Security	Bitdefender Install & SetUp	Bitdefender Antivirus Free Edition
Bitdefender Family Pack 2017	Bitdefender GravityZone Advanced Business Security	Bitdefender PC Optimizer	Bitdefender QuickScan
Bitdefender Total Security 2017	Bitdefender GravityZone Business Security	Bitdefender Virus & Spyware Removal	Bitdefender Adware Removal Tool for PC
Bitdefender Internet Security 2017	Bitdefender Security for Virtualized Environments	Bitdefender System Repair	Bitdefender Adware Removal Tool for Mac
Bitdefender Antivirus Plus 2017	Bitdefender Security for Mobile		Bitdefender Antivirus Free for Android
Bitdefender Antivirus for Mac			
Bitdefender Security for XP and Vista			
Bitdefender Mobile Security for Android			

© 2017, IJCSMC All Rights Reserved

Bitdefender Antispam NeuNet,[10] short for Neural Network is an antispam filter pre-trained by the Bitdefender Antispam Lab on a series of spam messages, so that it learns to recognize new spam by perceiving its similarities with the messages it has already examined. In May 2006 Bitdefender introduced a new technology, B-HAVE, to reduce dependency on virus signatures through proactive detection of unknown threats. This technology is based on behavioral analysis in a virtualized environment.

To determine whether a program is malicious or not, this technology makes use of a virtual PC in which files are executed and analyzed. The virtual PC includes a set of virtual hardware devices, mimicking the configuration of a typical PC. B-HAVE checks for characteristics known to be associated with malware. A program may be deemed to be malicious if it attempts to modify certain files, read from or write to a sensitive area of the memory or create a file that is a product of a known virus. When attempting to use a non-trusted program, B-HAVE delays the launching until the program's behavior and characteristics are analyzed and catalogued in the virtual environment. If no malicious actions are detected, B-HAVE starts the program normally; if a suspect conduct is present, B-HAVE automatically quarantines or deletes the application.[11] As of June 2007, Bitdefender had passed Virus Bulletin's VB100 independent tests 14 times out of 18 since first tested in 2002,[12] including the 12 most recent tests.[13] It also achieved an advanced certification from AV Comparatives for on-demand scanning,[14] and standard level certification for catching unknown viruses, though it was criticised for its slower scanning speed and higher instances of false positives.[15] In another test conducted by AV Comparatives in August 2009[16] to determine the antivirus software with high detection rates and the lowest false positives rating, Bitdefender received an Advanced+ Certification. In a test conducted by PCMag, BitDefender 2010, "detected 97 percent of all the threats and completely blocked installation for most of them".[17] In reviews for Bitdefender, the home version of the suite was given the PC Answers editor's choice award in a comparative review in May 2007.[18] It is also the least expensive of the top three antivirus solutions, as ranked by PC World. TopTenREVIEWS gave Bitdefender Antivirus Plus a 9.8 rating out of 10, and said "Bitdefender combines superb protection, ample features, and comprehensive support at a price that's lower than other high-ranked programs."[19] In May 2009, support was being criticized as being unresponsive.[20] Bitdefender responded by saying they were aware of the problems, and that they would take steps to solve it. They attributed the problem to an unexpectedly high surge in customers due to a positive review.[20] Currently, the company's website claims that support is available 24/7 on telephone, e-mail, Livechat, and an online knowledge base.[21] On March 20, 2010, computers running Bitdefender under 64-bit versions of Windows were affected by a malfunctioning update which classified every executable program as well as dll files as infected. These files were all marked as 'Trojan.FakeAlert.5' and were moved into quarantine. This action led to software and systems malfunctions that affected users around the world.[22] Bitdefender

© 2017, IJCSMC All Rights Reserved

representatives announced the removal of the faulty update and a workaround for the users affected,[23] except for those using the 2008 version.[24] As of version 2012 of Bitdefender, Comodo Firewall and Bitdefender cannot co-exist. There is however, a workaround which can be found elsewhere on the Internet and on the Bitdefender forums.[25] There are alternatives, such as TinyWall,[26] which are compatible with Bitdefender Antivirus (Bitdefender Internet Security and Total Security have a built-in firewall—it is recommended to only have one firewall installed; multiple firewalls may crash/slow-down the system). Bitdefender is incompatible with ASUS AiSuite2 and ASUS AiSuite3, a motherboard optimization suite of software bundled with ASUS motherboards which enables automatic overclocking, power tuning and fan control. Bitdefender claims that the incompatibility is due to "NDIS ASUS driver (WinpkFilter LightWeight Filter), which prevents the installation of some Bitdefender files".[27]

The aftermath of a successful attack

According to the computer security institute's annual computer crime and security survey, the average cost per incident is $300,000. don't be fooled into thinking that this number represents only the largest organizations. Close to a quarter of all those surveyed in this report were organizations that have between 1 - 99 employees. to a large company, losing $300,000 dollars can put a dent in the bottom line, but to a small business this loss can be devastating. web applications are used to process data and make it accessible to users across the internet. Whether the application is used to process credit cards, manage employees, or increase collaboration between partners, failing to protect these applications can have serious ramifications. Compliance issues - to ensure that organizations do what is necessary to protect confidential information, governments and industries alike have put in place certain requirements. us laws like the healthcare information portability and accountability act (HIPAA) are used to protect confidential health information. to protect credit card information, the payment card industry (PCI) has created its own set of requirements. Failure to comply with industry wide or governmental requirements often result in large fines waged against the organization responsible for protecting the information. data theft - in addition to personal and financial information being stolen, a large cost that organizations may face after having a web application compromised is the loss of proprietary information. Web applications process a great deal of personal information; however, they are also used for collaboration and project management. Organizations with offices across the globe need some way of working together and many web applications provide such a way. attackers know this, and often times the objective of their crime is to steal intellectual property either a corporate espionage or to sell to a competitor. customer/visitor loss of trust - this is one of the most intangible costs associated with a website being attacked; it is, at the same time, one that should be expected. when the tjx companies made the news because they were victimized by albert gonzalez, customers lost trust in their ability to protect their

© 2017, IJCSMC All Rights Reserved

credit card information. likewise, when google warns that a website is untrustworthy, even the most loyal visitors avoid the site for fear of having their information stolen or their computer infected burden on resources - not all attacks are launched with the intent of profitin directly. attackers still launch denial of service attacks against websites to disrupt service to legitimate visitors. Additionally, compromised web servers and sites are used to host multimedia files, malicious files, and links to other websites without the knowledge of the owner. in these instances, storage space and bandwidth are wasted on illegitimate use. ability to attack the internal network - those organizations who host their web servers on site risk having one of their applications serve as a entry point to the internal network where other servers, databases, and computers can also be compromised. going right through the vulnerabilities in these applications bypasses any network perimeter defenses put in place.

How to create a Firewall zone in Bitdefender

Depending on the network you are connected to, the Bitdefender Firewall may block the connection between your system and another device (such as another computer or a printer). As a result, you may no longer share or print files. In this case, make sure that the Firewall settings are allowing the PC communication with the respective device: 1.Open Bitdefender, go to the **Protection** panel and select the **Firewall** option

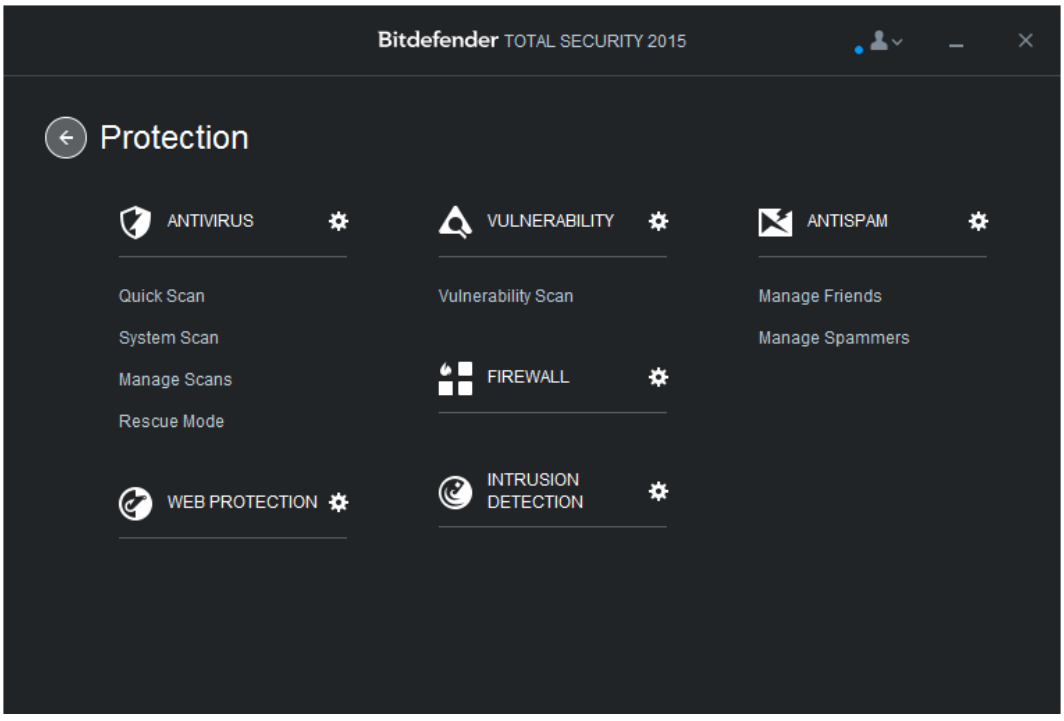

Fig (1) Bitdefender interface

© 2017, IJCSMC All Rights Reserved

2. In the Firewall section select the **Adapters** tab from the top and locate the adapter. It is either Local Area Connection if the device is connected by cable or Wireless Area connection if it is a wireless device.

3. Click on the small arrow next to each information displayed for this network connection. A drop-down menu appears. Set:

- **Network Type** to **Home/Office**
- **Stealth Mode** to **Off**
- **Generic** to **Yes**

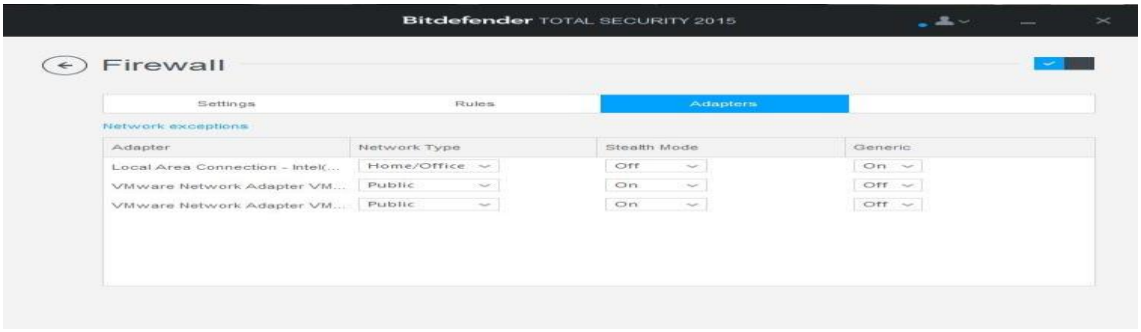

Fig (2) Firewall interface

Check if the issue persists. If it does, the best solution is to configure Bitdefender to automatically allow connections to and from the respective device. For each network connection you can configure a special network exception.

To add a network exception on your adapters, follow these steps:

1. Open the Bitdefender window.

2. Click the **Protection** section.

3. In their select the **Firewall**.

4. In the **Firewall** window, select the Adapters tab.

5. In here you will find highlighted in blue the Network exceptions option.

6. Once you access it, you can type in the **Address** field the IP. You can also select here for which one of the connections you wish the setting to be applied and its permission type: **Allow** or **Deny**.

7. After you make the proper selections, just click on the blue button with a plus (+) sign on it for the exception to be created.

© 2017, IJCSMC All Rights Reserved

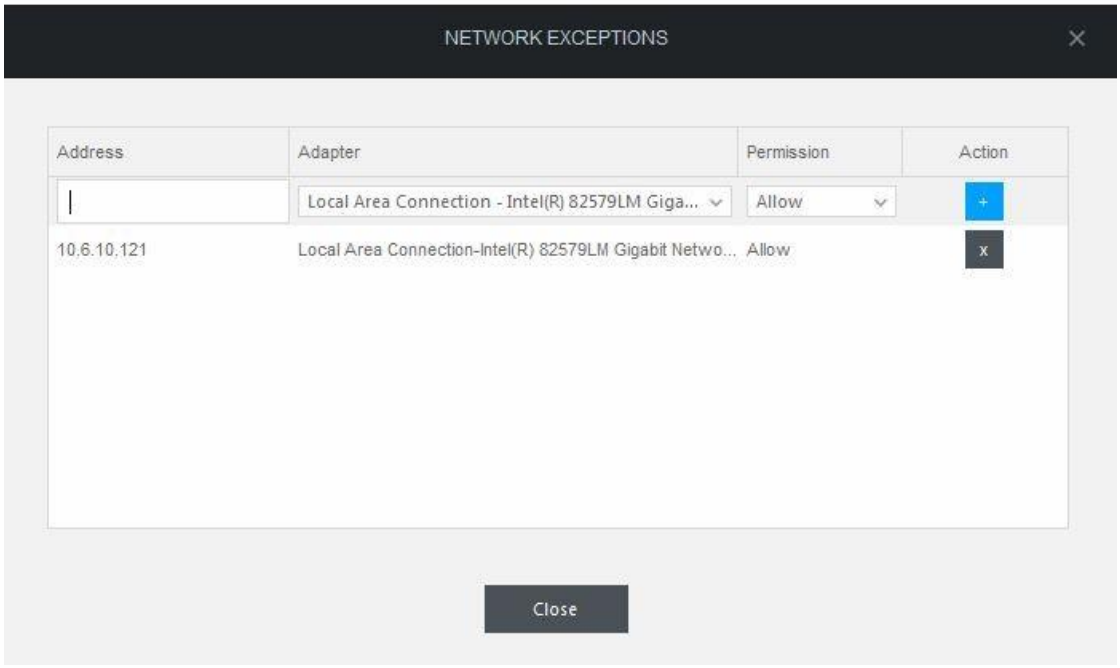

Fig (3) Protection section

References

1. **"Bitdefender Partners with Slovenia's Kron Telekom to Expand Sales". bitdefender.com. 29 September 2014. Retrieved 2016-01-10.**
2. **Softwin SRL, avx@softwin.ro. "Antivirus eXpert". Securityfocus.com. Retrieved 2010-11-09.**
3. **"Bitdefender Antivirus Plus 2017 Review". AntivirusProtection.reviews. Retrieved 2017-04-06.**
4. **"Gartner Magic Quadrant for Endpoint Protection Platforms".**
5. **"Bitdefender Products for Home Users".**
6. **"Bitdefender Business Solutions".**
7. **"Technical Support Services - Bitdefender Tech Assist". www.bitdefender.com. Retrieved 2017-02-20.**
8. **"Bitdefender Free Tools".**
9. **Bitdefender Antispam NeuNet**
10. **"B-HAVE – The Road To Success". Security-int.com.**
11. **"Virus Bulletin: VB100 Results - Bitdefender (SOFTWIN)". Archived from the originalon April 3, 2008.**
12. **Rubenking, Neil J. (2015-09-15). "Bitdefender Antivirus Plus 2016". PCMAG. Retrieved 2015-10-15.**
13. **"Anti-Virus Comparative February 2007".**
14. **"BitDefender Antivirus 10 review". PC World. 2007-04-23. Retrieved 2012-10-27.**
15. **"Anti-Virus Comparative August 2009" (PDF). Retrieved 2010-11-09.**
16. **Rubenking, Neil J. (2009-08-17). "'PCMag BitDefender Total Security 2010'". Pcmag.com. Retrieved 2012-10-27.**

© 2017, IJCSMC All Rights Reserved

17. "Group Test: AV Software" (PDF). PC Answers magazine. Future Publishing. May 2007. pp. 118–125. Archived from the original (PDF) on April 24, 2007.
18. "Best Antivirus Softwarez Review 2014". Retrieved 2014-04-24.
19. . Pcworld.com. Retrieved 2010-11-09.
20. "Support Center". Bitdefender.com. Retrieved 2010-11-09.
21. McMillan, Robert. "Bad BitDefender Update Clobbers Windows PCs". PC World.
22. "Trojan.FakeAlert.5 Update issue".
23. Peter Bright (2010-03-22). "BitDefender update breaks 64-bit Windows PCs".
24. "2012 Not Compatible With Comodo Firewall - Bitdefender Forum". Forum.bitdefender.com. Retrieved 2013-07-11.
25. http://tinywall.pados.hu/
26. "Bitdefender installation fails due to ASUS AI Suite software - Bitdefender Support Centre". bitdefender.co.uk. Retrieved 2014-06-04.

© 2017, IJCSMC All Rights Reserved