ISSN 2320-9984

Volume 3 Issue 1 | March 2015 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

A Novel Methodology for Web Browser

Ashish Sahu
Research Scholar
Adina Institute of Science and Technology
Sagar (M.P.), [INDIA]
Email:ashish_sahu5555@radiffmail.com

Satyam Soni
Research Scholar
Adina Institute of Science and Technology
Sagar (M.P.), [INDIA]
Email:sonisatyam325@gmail.com

Raksha Chaurasiya
Research Scholar
Adina Institute of Science and Technology
Sagar (M.P.), [INDIA]
Email:rakshachourasiya0@gmail.com

Abhishek Keserwani
Assistant Professor
Department of Computer Science & Engineering
Adina Institute of Science and Technology
Sagar (M.P.), [INDIA]
Email: abhishekk8.adina@gmail.com

Abstract—*In this paper, we introduce the security issues in functionality extension mechanisms supported by web browsers. Extensions (or "plug-ins") in modern web browsers enjoys lots off power without restraint and thus are attractive vectors for malware. To confirm the claim, we take on the role of malware writers looking to assume control of a user's browser space. We have taken advantage of the lack of security mechanisms for browser extensions and have implemented part of malware for the popular Firefox web browser, which we call BROWSERSPY, which requires no special privileges to be installed. Once installed, BROWSERSPY takes complete control of a user's browser space while being undetectable through the browser can inspect all activities performed. We then discussed strategies to protect against malware that adopt the role of defenders. Our primary contribution to the expansion of the installation and to control the process of loading code integrity checking technology that uses a mechanism. We set up a foundation to protect the dangers of extensions that provide extended runtime behavior monitoring techniques discussed.*

Keywords:—*plug-ins, browser, malware, debugging, information technology.*

1. INTRODUCTION

Internet web browser on a computer connected to a network, arguably the most used applications, today's computers have enabled millions of users a fast and is becoming crucial stage. Web browser email correspondence, shopping, social networking, personal finance management, and a wide range of activities, including professional business to provide an interface to perform, often a user's window to the world. Using the browser gives it a unique perspective; During the inspection and very personal activities relevant to the sensitive information provided by users meaning can apply. In addition, the browser user all incoming and outgoing communication encrypts, even when this information has reached clear. Sensitive, personal data warrant this high level of use in its efforts to ensure full confidentiality and integrity. A browser based on the code of confidentiality and integrity to ensure that safety concerns addresses a daunting task. For example, the browser's current distribution C, C ++, Java, JavaScript and XML that includes the 3.7 million lines of code written in various languages, building size (kloc as measured using the device have). The size and diversity of language implementation challenges it difficult for the problem of a "one stop shop" solution enables to develop. In this paper, we are in the presence of browser extensions in a browser to ensure confidentiality and integrity is equally important to focus on the sub-problem. We have about 70 million web users used by Mozilla Firefox, widely used in the free (open source) software, the browser, in the context of the problem discussed. Browser extensions (or "Add-ons") to customize the browser provided facilities. These extensions to change the behavior of the browser plug-ins, browser and other export interface using. Although Firefox is set up platform-specific (such as Windows XP, Linux or Mac OS X as one), extensions mainly platform-independent JavaScript and XML, is used to implement the major languages of the neutral nature are based on. Extensions to plug directly into the browser, however, to provide protection against malicious extensions in Firefox there is no provision at present. The load code that prevents any expansion started in debugging mode. However, in normal mode for specific installation and performance allow extensions to be executed. Who use them to many thousands of users, its download numbers as proof of the popularity of extensions, providing useful functionality. He dismissed concerns about the safety of the extension by closing ignores problems. To understand the impact of having a malicious extension, we really set a goal of crafting. Surprisingly, we have at least three weeks with minimal effort, sand, BROWSERSPY call a malicious extension engineer for the Firefox browser. Once installed, the extension takes full control of the browser. As further evidence, a recent extensive media coverage of the attack and inexperienced users have to worry about the form of a detective known as malware, use the Firefox browser extension, which was started on. User data confidentiality and integrity: to expand our presence and Form spy malware are two main problems raised by the extension. We extend our browsing, while sensitive data input by a user to a remote site to collect and display it from being logged. In this paper we present techniques that deal with these problems. Extension to address integrity, our solution code installation of malware threats, disallowing integrity there, as part of the browser is selected to run, with full control of the process by which the end user can do is. It detects and end-users are not authorized by the execution of the extension has refused to allow the user-authentication process is done by. Data confidentiality and integrity to address the second challenge, we put Spider Monkey JavaScript engine and other means that the extension of the state system based on a policy to enhance the browser with support for monitoring.

2. RELATED WORK

Firefox, Internet Explorer (IE), Safari and Opera: We examined four contemporary browsers support the expansion. We have studied the four between browsers, only Safari browser does not support the concept of extension. The remaining three extensible architecture officer, but the expansion is not based protection mechanisms to address threats. For example, the primary extension mechanism IE Browser Helper Object (BHO) is through. Pest Patrol website malware detection in Windows Vista as "protected-mode browser as" In addition, the browser used in the integrity and confidentiality of personal data to the end user is not addressed in the recent mechanisms that use BHOs Hundreds of malware lists. Securely to the problem of running in a browser extension download an operating system executing untrusted code to the problem is similar in many ways. It is a well-known problem, and research ideas in code, static analysis, proof-carrying code, model-carrying code and performance monitoring approach has led such as signed. Below, we have highlighted several technical and practical reasons, the applicability of the browser extension issue discussed. Signed code-signed the Firefox browser offers support for extensions; although it is rarely used in practice. Extensions and only two have been signed. In addition, we signed the extension, only the first level of protection proposed that note. They are only distributing the browser and do not guarantee unmodified in transit; No assurance about the security implications of running the extension is provided. Static analysis of code to implement policies on expanding the use of static analysis is very desirable approach. Static analysis to identify vulnerabilities or malicious intent, many past efforts has been employed. The primary advantage of using static analysis, dynamic analysis based solution embodies the performance and the absence of the upper sequence stops are. This, however, without making conservative assumptions for JavaScript code static analysis is difficult to employ. His approach like the above scenario is a conservative form of tainting is controlled. In scenarios that require data to order Congress to employ specific approach is:

1. Check with the original script change order That travel safety applicable property

2. Conversion program that respects the property to produce a proof.

3. CONCLUSIONS

We have security concerns that exist in modern extensible web browser as a proof of concept malicious extension authors. It suffers because of these flaws, many open-source browser Firefox as our target platform selected.

The threat of malicious extension was addressed using two mechanisms:

Extension set is valid on the integrity by which :

1. A mechanism Load time Surveillance order further attacks on the browser core integrity and confidentiality of sensitive data to implement a policy to prevent the extension.
2. Infrastructure Our change to Firefox browser which allows a user to load only extensions installed, and detects unauthorized changes made to the installed extensions that insurance. The amendment to an external standard browser session and type of injection installations disallowing vector seals set out for malicious extensions. We monitor a significant portion of the code in order to expand and implement policy on a per -extension enabled browser.

REFERENCES :

[1] Goldberg, D. Wagner, R. Thomas, and E. A. Brewer. A secure environment for untrusted helper applications: confining the wily hacker. In USENIX Security Symposium, 1996.

[2] O. Hallaraker and G. Vigna. Detecting Malicious JavaScript Code in Mozilla. In Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems (ICECCS), pages 85–94, Shanghai, China, June 2005.

[3] J. Kirk. Trojan cloaks itself as firefox extension. Infoworld magazine, July 2006.

[4] B. W. Lampson. A note on the confinement problem. Communications of the ACM, 16 (10), 1973.