doi :10.3969/j.issn.1671-1122.2012.08.005

恶意浏览器扩展行为分析与建模

王雷，张令臣，向继，余幸杰

（中国科学院信息工程研究所信息安全国家重点实验室，北京 100093）

摘 要：文章基于开源的 Firefox 浏览器，对运行于 Firefox 内部的浏览器扩展的行为进行分析、总结，对恶意浏览器扩展的行为进行分类，并建立恶意浏览器扩展的状态转移行为模型，以对恶意浏览器扩展的恶意行为进行较为全面的描述，为后续针对恶意浏览器扩展的检测工作奠定基础，以期建立和完善安全浏览器。

关键词：Firefox；浏览器扩展；行为分析；状态转移模型

中图分类号：TP393.08 文献标识码：A 文章编号：1671-1122（2012）08-0015-03

Modeling and Analyzing the Behavior of Malicious Browser Extensions

WANG Lei, ZHANG Ling-chen, XIANG Ji, YU Xing-Jie

(*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing,* 100093 *China*)

Abstract: Based on the open-source browser, Firefox, we investigate into the behavior of the browser extensions which are executing within Firefox, and classify the malicious browser extensions into four categories and propose the state-transition-based behavior model of the malicious ones to depict their behavior more concretely. It is the foundation of our future work on detecting the malicious browser extensions and realizing the secure browser tool.

Key words: Firefox; browser extensions; behavior-based analysis; state transition model

0 引言

网页浏览器工具的发展，改变了早先仅仅对于 HTML 语言文档解析的单一功能，已经发展成显示丰富的多媒体内容，可与用户交流、互动的网页内容工具。浏览器工具在增加自身功能的同时，也增加了对于浏览器扩展、插件的支持，以进一步丰富浏览器的功能。Mozilla Firefox 浏览器作为一个开源的项目，使得开发者和程序爱好者能够更加容易地扩展 Firefox 浏览器的功能。编写浏览器扩展的形式，不仅对浏览器功能进行了扩充，也使得浏览器扩展可以运行于多种操作系统平台的 Firefox 浏览器中，因此更具跨平台性，这也是深受程序爱好者青睐的重要原因。

随着浏览器扩展、插件在浏览器中的广泛使用，在扩充浏览器功能的同时，也带来了新的安全问题，同 Microsoft IE 浏览器的 BHO 插件的安全问题一样，由于误用、滥用浏览器扩展，恶意代码可能秘密地执行一些恶意的操作，危害用户数据安全。安装于 Firefox 浏览器内的浏览器扩展，可以获得与 Firefox 浏览器相同的访问控制权限，因此浏览器扩展除了能够完成其声称的功能，还能够做更多的事情，如访问用户主机本地文件系统，并且拥有读、写、执行的权限；访问网络通信系统，与远程服务器建立套接字进行通信；创建新的进程，甚至阻挡一个正在运行的进程等，这都使得浏览器扩展受到攻击者的关注，从而引发许多安全问题。

本文在对浏览器扩展的组成、运行原理研究的基础上，分析、总结恶意浏览器扩展的行为特点，并建立基于状态转移的行为模型，进而对恶意浏览器扩展的攻击行为进行详细地描述，为针对恶意浏览器扩展的行为分析与检测技术的研究提供基础。

1 浏览器扩展研究

浏览器在最早出现的时候，仅仅用来显示静态的 HTML 文本、图片等简单的信息，但是随着计算机技术和网络技术的发展，人们对浏览器的要求也在不断地增大，要求浏览器能够支持显示网页游戏等复杂功能。传统的浏览器已经不能够满足用户需求，

收稿时间：2012-07-12

基金项目：中国科学院战略性先导专项 [XDA06010702]、国家自然科学基金 [70890084/G021102、61003274]

作者简介：王雷（1985-），男，河北，博士研究生，主要研究方向：网络与系统安全；张令臣（1986-），男，山东，博士研究生，主要研究方向：Web 安全、云计算安全；向继（1976-），男，湖北，高级工程师，博士后，主要研究方向：网络与系统安全、Web 安全、网络存储安全；余幸杰（1988-），女，湖南，硕士研究生，主要研究方向：云计算安全。

也就出现了多种插件、扩展程序，用来扩充浏览器的功能，使浏览器进一步满足用户的需求，同时也给用户带来方便，提高用户的浏览体验。

在本文中，我们选用 Firefox 浏览器作为研究对象，本节主要对 Firefox 浏览器的扩展程序进行分析与总结，叙述 Firefox 浏览器扩展的基本组成与运行原理。

Firefox 浏览器扩展根据其实现语言的不同，主要有 JavaScript 扩展、C++ 扩展和 Python 扩展。其中，JavaScript 扩展使用最为广泛，Mozilla 为其维护了一个官方的发布网站 AMO[1]，供程序开发者上传浏览器扩展，并经过审核之后，在 AMO 网站上发布并提供下载。

JavaScript 浏览器扩展 [2]，主要由 chrome.manifest, install.rdf, chrome package, defaults package 组成，而 chrome package 里面包含 content, skin, locale packages。但简单的浏览器扩展 [3]，有时在扩展的文件夹中，仅仅拥有 chrome.manifest, install.rdf, content package。

1）chrome.manifest 是浏览器扩展进行 chrome 注册的清单文件，用于在 Firefox 内部进行注册；2）install.rdf 包含了浏览器扩展安装的信息；3）content 目录下面存放的是浏览器扩展用于描述界面的 XUL 文件和增加行为的 JavaScript 文件，XUL 文件将会制定浏览器扩展在 Firefox 中运行时表现的界面和功能；4）locale 目录存放的是本地化相关的文件；5）skin 目录存放的是一些 CSS 文件，用来定义浏览器扩展的外观，通常包含 CSS 文件和图像文件。

浏览器扩展通过调用 Firefox 提供的 API，即 XPCOM 组件 [4]，完成其相应的功能。浏览器扩展在 Firefox 中运行时，与网页中的 JavaScript 代码、浏览器自身的 JavaScript 代码一样，由 Firefox 浏览器内嵌的 JavaScript 引擎 SpiderMonkey[5] 进行编译运行，chrome.manifest 通知 Firefox 浏览器加载 overlay、content 等目录，执行 XUL 文件。通常 JavaScript 文件是在 XUL 文件中引入调用，而 JavaScript 代码又通过 Firefox 提供的 XPConnect[6] 访问 XPCOM 组件接口，完成相应功能。

Firefox 浏览器扩展的运行模式，是根据发生的事件进行响应，从而完成相应功能。例如，可以利用 window.addEventListener() 函数在 Firefox 中设定响应的事件，同时在 JavaScript 代码文件中定义事件响应发生的行为，即功能函数，从而实现 Firefox 浏览器扩展的功能。

2 恶意浏览器扩展行为分析与建模

2.1 恶意浏览器扩展行为分析

比较常见的恶意浏览器扩展主要包含以下几种情况：

1）篡改已经安装的合法浏览器扩展。BrowserSpy[7] 是嵌入在 Google Toolbar 中实现的一个恶意的浏览器扩展，它可以获取存储于 Firefox 口令管理器中的口令，获取浏览历史记录，截获用户在网页中输入的信用卡账号等敏感数据信息。由于 Firefox 浏览器仅仅在第一次安装浏览器扩展的时候检查其完整性，而在后续运行过程中并没有检查浏览器扩展的完整性，因此文献 [7] 的作者在已经发布的、合法的浏览器扩展 Google Toolbar 中添加恶意的 JavaScript 脚本代码，实现了 BrowserSpy 的恶意攻击行为。因此，通过篡改安装于 Firefox 浏览器中的浏览器扩展，也可以实现恶意浏览器扩展的攻击，危害用户数据信息安全。

2）存在漏洞的浏览器扩展。2007 年，广泛使用的 Firefox 浏览器扩展 Firebug[8] 被发现存在多个漏洞。如果攻击者利用 Firebug 的漏洞，构造含有攻击代码的网页，那么当安装有 Firebug 的 Firefox 浏览器访问这一网页时，具有攻击行为的脚本代码就会在“ chrome ”上下文环境中运行，它拥有与 Firefox 浏览器相同的访问权限，能够做许多事情，而不像网页中的脚本代码受到一些限制，如 SOP 准则 [9] 的限制。例如，攻击者可以利用浏览器扩展的漏洞，自动去某个特定的 URL 下载并安装事先准备的二进制恶意代码，并自动运行于用户主机，达到攻击的目的。

2.2 典型的恶意浏览器扩展举例[8]

1）FFSniFF 是最早出现的 Firefox 恶意浏览器扩展之一。虽然其实现的功能比较简单，仅仅是获取用户在网页中输入的口令信息，并且将获取到的口令信息以邮件的形式发送给攻击者。在 Firefox 的扩展管理器中无法得知是否已经安装了 FFSniFF 扩展，当用户使用 Firefox 浏览器进行网页浏览时，FFSniFF 浏览器扩展会自动运行，并进行信息窃取行为。

2）Trojan.Brojack 同样利用了浏览器扩展的可隐藏特性，并不在浏览器扩展管理器中显示，同时它自动创建 DLL 文件，以作为 Microsoft IE 浏览器的 BHO 插件，供 IE 浏览器使用。从而收集 Firefox 浏览器和 IE 浏览器的历史记录，并将收集到的数据传送给远程服务器。

3）Infostealer.Snifula 将自己在 Firefox 中伪装成一个合法的浏览器扩展“ NumberedLinks v0.9 ”，从而蒙蔽用户，使得用户误以为它是合法的浏览器扩展，记录用户在网页中输入的口令信息以及其他敏感信息，并将获取的敏感数据信息发送给远程服务器，达到信息窃取的目的。

4）Adware.MyCentria 通过程序“ installFF.exe ”安装于 Firefox 浏览器，这个扩展能够检查用户浏览器的网页信息，从而在用户浏览特定网页时，自动下载广告信息呈现在网页中。该扩展以用户常用的搜索引擎作为攻击目标，将自动下载的广告信息与搜索的网页内容一同呈现给用户，以掩盖它自己的广告下载行为。

5）Trojan.Hanambot 在安装于 Firefox 之后，首先清除浏

览器全部的 Cookie 信息，然后在用户浏览网页的时候，获取网页的 URL，并且利用正则表达式匹配规则，与攻击者事先定义的 URL 信息相比较。如果发现用户访问的是银行网页，那么就记录浏览器的 Cookie 信息、用户的账户登录信息等，并将这些获取到的信息提交给远程服务器。此外，Trojan.Hanambot 在安装浏览器扩展的同时，还在用户主机上安装了 Rootkit 程序，以接收僵尸网络命令，使用户主机成为僵尸网络的一员。

针对恶意的浏览器扩展，Mozilla 在 AMO 网站上维护了一个黑名单列表 [10]，用以提醒用户历史上出现的恶意浏览器扩展，以防止用户再次下载恶意浏览器扩展，从而威胁用户信息安全，同时在 Firefox 发布的更新版本中，自动禁止已经出现在黑名单中的浏览器扩展在 Firefox 浏览器中运行。虽然 Mozilla 黑名单上存在多个恶意的浏览器扩展程序，但是目前黑名单上的浏览器扩展程序已经无法下载。

2.2 恶意浏览器扩展行为模型

通过对上述恶意浏览器扩展的分析与研究，以及借助于恶意二进制代码程序的攻击行为的分析，我们将恶意的浏览器扩展分为四类：

1）信息窃取浏览器扩展，这类浏览器扩展窃取用户在网页中输入的用户名 / 口令，窃取用户计算机中存储的敏感信息、注册表信息等，如 FFSniFF；

2）恶意广告浏览器扩展，该类浏览器扩展自动下载广告信息，并在用户浏览的网页上进行播放，称之为 Adware；

3）恶意程序下载浏览器扩展，这类浏览器扩展自动从 Internet下载病毒、木马等恶意程序，并自动执行，给用户主机造成影响，危害用户主机安全；

4）恶意篡改内容浏览器扩展，这类浏览器扩展劫持用户网页浏览会话，恶意篡改会话内容，导致用户浏览失败，或者浏览网页被篡改。

通过对恶意浏览器扩展的行为分类，我们基于浏览器扩展在运行时调用的 XPCOM 组件资源序列，建立恶意浏览器扩展状态转移行为模型$A=(Q,\Sigma,\delta,s,F)$。其中，

1）状态集合 Q={ 初始状态 S_0，敏感信息读取状态 S_1，数据下载状态 S_2，数据保存状态 S_3，会话劫持状态 S_4，读取下载中间状态 S_{12}，读取劫持中间状态 S_{14}，下载劫持中间状态 S_{234}，读取下载劫持中间状态 S_{124}，读取下载保存中间状态 S_{123}，下载保存劫持中间状态 S_{234}，读取下载保存劫持中间状态 S_{1234}，敏感信息窃取浏览器扩展状态 S_6，文件下载执行浏览器扩展状态 S_7，广告数据下载浏览器扩展状态 S_8，会话信息篡改浏览器扩展状态 S_9}

2）输入字母表$\sum$ ={ 敏感信息读取操作 α，网络数据下载操作 γ，网络会话劫持操作 δ，数据信息网络发送操作 μ，网络数据保存操作 ε，内容播放操作 ζ，网络会话篡改操作，文件运行操作 η}

3）开始状态 s={ 初始状态 S_0}

4）接收状态集合 F={ 敏感信息窃取浏览器扩展状态 S_6，文件下载执行浏览器扩展状态 S_7，广告数据下载浏览器扩展状态 S_8，会话信息篡改浏览器扩展状态 S_9}

5）转移函数 δ 由下面的状态转移表 1 定义。

该恶意浏览器扩展状态转移行为模型，能够对恶意浏览器扩展的一般行为进行描述。行为模型中的状态都是浏览器扩展在 Firefox 内部运行时所访问的、可能被攻击者利用来发起攻击，威胁用户数据信息安全的 XPCOM 组件资源，因为这些 XPCOM 组件调用序列能够对浏览器扩展的行为进行描述与刻画。同时，这个状态转移行为模型，可为恶意浏览器扩展行为分析检测技术的研究提供技术支持。

3 结束语

在本文中，我们通过对恶意浏览器扩展的行为分析，将恶意浏览器扩展进行了分类，同时建立了基于状态转移的恶意浏览器扩展行为模型，用以描述、刻画恶意浏览器扩展在 Firefox 浏览器中运行时的攻击行为。本文的研究内容对恶意浏览器扩展的行为特征描述提供基础，下一步工作是研究针对恶意浏览器扩展的行为分析检测技术，以建立安全的浏览器系统，保证用户的数据安全。（责编 程斌）

参考文献：

[1] AMO: Addons.Mozilla.Org [EB/OL]. https://addons.mozilla.org, 2012.

[2] Firefox 扩展相关代码分析报告 [EB/OL]. http://wenku.baidu.com/view/4eac4c1bfc4ffe473368abc9.ht- ml, 2009-12-16.

[3] Mozilla Developer Network. Building an Firefox Extension [EB/OL]. https://developer.mozilla.org/e- n/Building_an_Extension, 2012.

[4] Mozilla Developer Network. XPCOM [EB/OL]. https://developer.mozilla.org/en/XPCOM, 2012.

[5] Mozilla Developer Network. SpiderMonkey [EB/OL]. https://developer.mozilla.org/en/SpiderMonkey, 2012.

[6] Mozilla Developer Network. Mozilla XPConnect [EB/OL]. https://developer.mozilla.org/en/XPConne- ct, 2012.

[7] A. Holzammer. Security Issues about Web Browser Add-ons [R]. Seminar Internet Sicherheit, Technisc-he Universit at Berlin, 2008.

[8] Elia Florio CandidW ü est. Firefox and Malware: When Browsers Attack [R]. Symantec Corporation Whitepaper, 2009.

[9] J. Ruderman. SOP: The Same-Origin Policy [EB/OL]. http://www.mozilla.org/projects/security/comp- onents/same-origin.html, 2001-08.

[10] Mozilla Addons Blocklist [EB/OL]. http://www.mozilla.com/en-US/blocklist/, 2012.

恶意浏览器扩展行为分析与建模

作者： 王雷， 张令臣， 向继， 余幸杰
作者单位： 中国科学院信息工程研究所信息安全国家重点实验室,北京 100093
刊名： 信息网络安全
英文刊名： Netinfo Security
年，卷(期)： 2012(8)

参考文献(10条)

1. AMO: Addons.Mozilla.Org 2012

2. Firefox扩展相关代码分析报告 2009

3. Mozil a Developer Network Building an Firefox Extension 2012

4. Mozil a Developer Network. XPCOM 2012

5. Mozilla Developer Network SpiderMonkey 2012

6. Mozil a Developer Network Mozil a XPConnect 2012

7. A.Holzammer Security Issues about Web Browser Add-ons 2008

8. Elia Florio CandidWüest Firefox and Malware:When Browsers Attack 2009

9. J. Ruderman SOP: The Same-Origin Policy 2001

10. Mozilla Addons Blocklist 2012