This research article is a short technical publication focused on technical approach used from attackers.

Because the attack campaign is "ALIVE" I will not revel the real IP addresses and the real name of the targeted bank.

Are 2 factor authentications enough to protect your money?

Targeting Italian Bank and Customers

ABSTRACT

During our recent analysis of malware targeting financial institution we found a very powerful that can bypass the 2FA (Two factor-authentication) with a malicious app installed on the phone. Malware like this can drive the user to download the fake application on the phone, using a MITB (Man in the browser attack). Once the user PC the attacker can take full control of the machine and interact with him through a C&C server. What we explain in this article is a real active botnet with at least 40-compromised zombie host.

SERVER INFO

The server used like C&C center to control the "bots" is located in France with following info.

- **Domain**: https://xxx.net
- **Url**: https://xxx.net/xxx/index.php
- **IP Address**: 95.XXX.XXX.XX or 176.XX.XXX.X
- **IP Location**: France
- **Associated mail**: sxxxxxxxx@gmail.com
- **Reverse DNS**: XXX
- **IP Blacklist Check**:

blocklist	link	status	description
red			
bl.spamcannibal.org	link	(127.0.0.2) bl.spamcannibal.org	
timeout			
combined.njabl.org			
dnsbl.njabl.org			
b.barracudacentral.org	link		
relays.mail-abuse.org	link		?
dev.null.dk	link		?
blackholes.mail-abuse.org	link		?
rbl-plus.mail-abuse.org			
dnsbl.ahbl.org	link		
opm.blitzed.org	link		
access.redhawk.org			
bl.technovision.dk			
korea.services.net			
exemptions.ahbl	link		

- **ASN**: ASXXX76

Figure 1: Network details

This research article is a short technical publication focused on technical approach used from attackers.

Because the attack campaign is "ALIVE" I will not revel the real IP addresses and the real name of the targeted bank.

Figure 2: IP Geolocation

Graph

The graph shows an easy to understand visual presentation of the different records associated with a domain

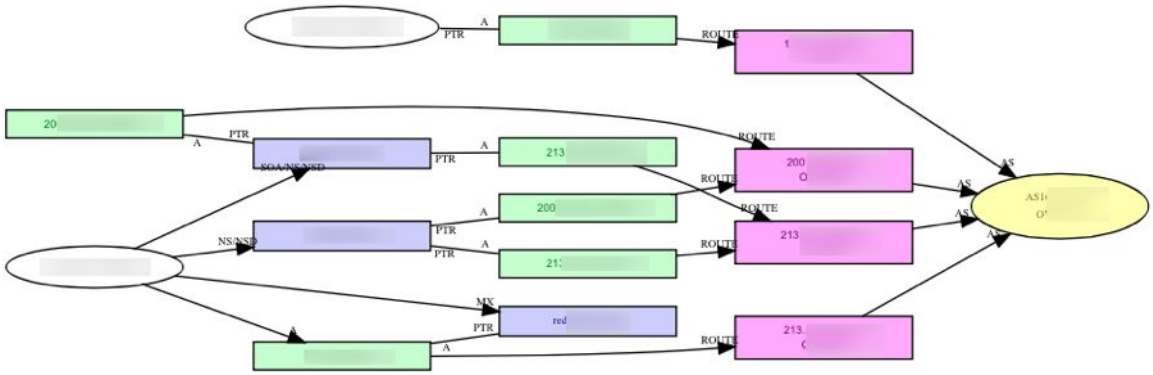


Figure 3 Graph

Records

Displays various information related to AS, BGP, Routes and Location.

Base	Record	Preference	Name	IP Number	Reverse	Routes	AS	Location
	A							France
	NS (primary)							
	NS							France
	MX	1						France

Figure 4 Records

HOW THE 2FA IS BYPASSED

During the last days we are seeing criminals developing more sophisticated solutions and have increasing knowledge in mobile and web programming. This scenario is increasing in the entire world and mostly in Europe. Criminals are developing solutions to bypass the 2FA used by the 90% of banks developing "legal" application published in the Google Play Store and Apple App Store. These applications can steal information on the phone, intercept and send it over the network silently. The last operation named "Operation Emmenthal", discovered by Trend Micro is acting in this way. In this section we will discover how a criminal can force a user to download and install the mobile application.

When a malware infects the machine and user navigate to the online banking platform, a MITB attack start, injecting JavaScript code inside the browser. This injection modifies some data in the page while keeping the same structure. During the navigation the hacked website will invite the user to download the fake application, explaining all the steps to insert their data. The app can be downloaded in two different ways:

- SMS (inserting your number in the fake form you will receive an SMS with the download link from the store)

Figure 5 Sms sent by attackers to download the apk

- QR Code

Figure 6 QR Code used to download the apk

After the user read the QR code or click on the link received by an SMS, he will be directed to the Google Play Store to download the application. Here is the screenshot of that process.

Figure 7 Step 1 to install the application.

This research article is a short technical publication focused on technical approach used from attackers.

Because the attack campaign is "ALIVE" I will not revel the real IP addresses and the real name of the targeted bank.

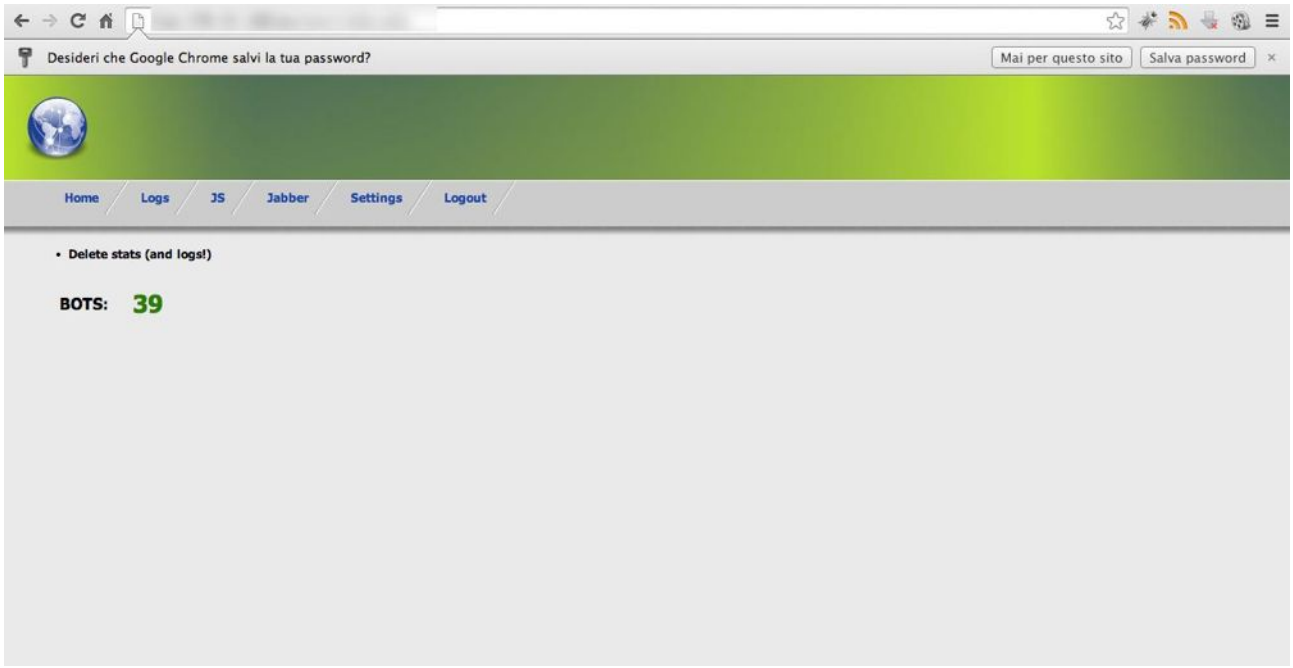
Figure 8 Step 2

Figure 9 First screen of the mobile application

C&C CENTER FUNCTION DETAILS

During our code analysis we found a link to a JavaScript file used by criminals during the injection process in the MITB attack. Going deeply in the obfuscated code we found a link to a C&C server where data are sent. Behind the front-end which was password protected we saw a custom control panel used to control the botnet. Every single bot is represented in a table and is controlled with the panel.

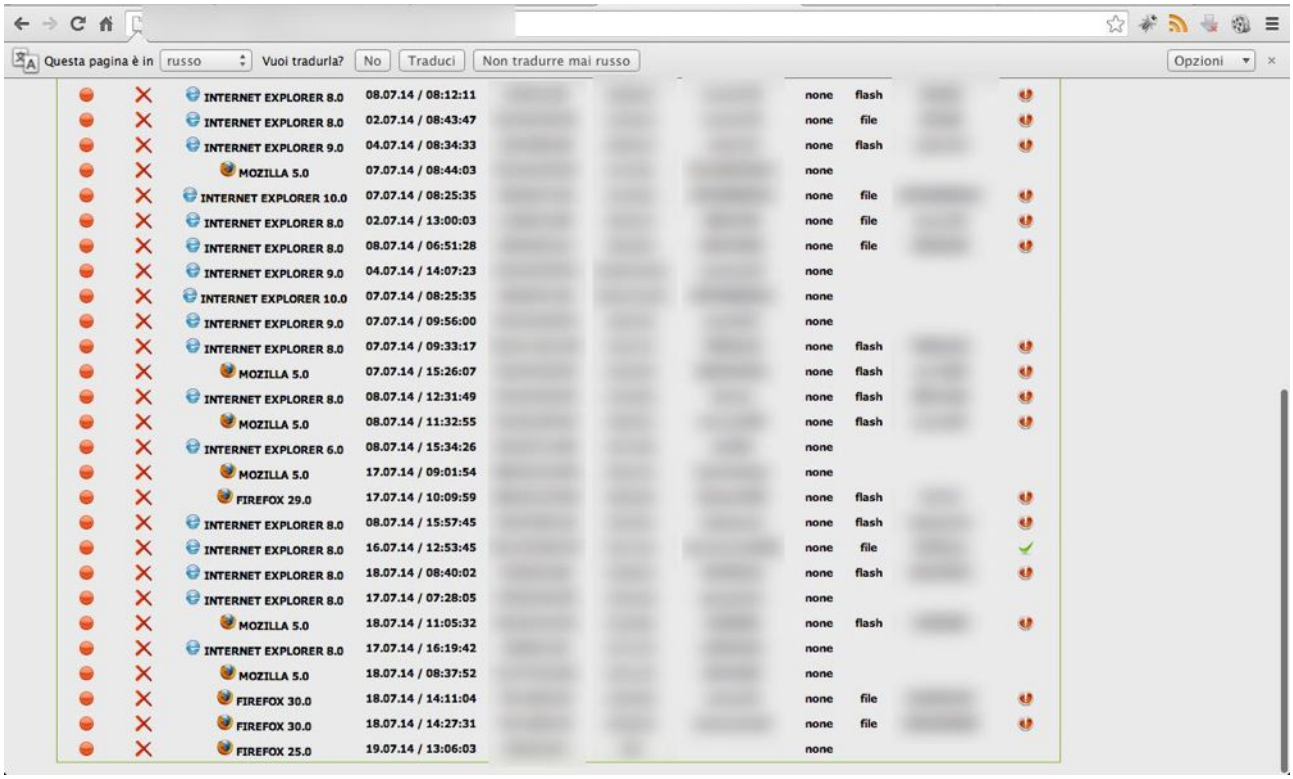
The fist screen you can see behind the login panel is a statistic page with the number of compromised hosts.



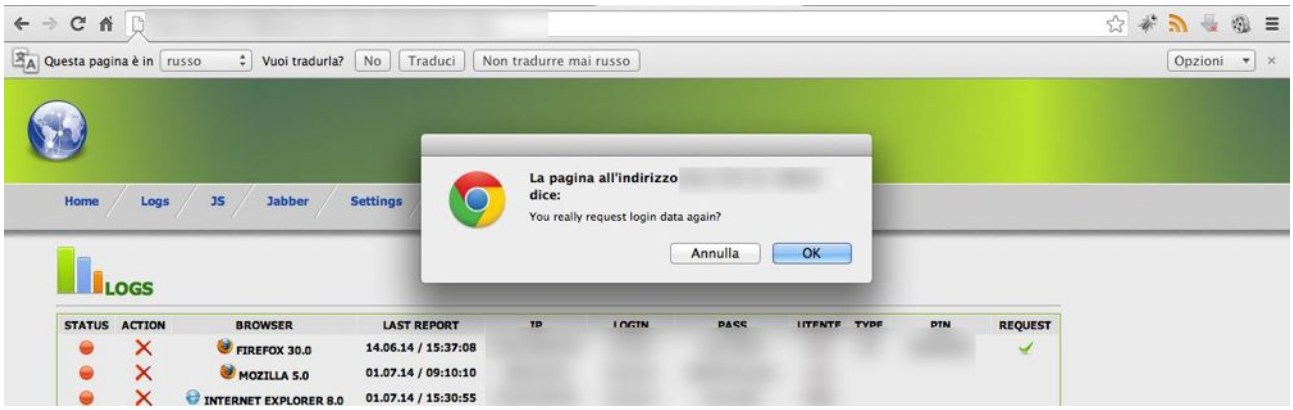
In the second one (Logs) there is all the information about bots:

- Used browser
- Last operation on that bot
- IP
- Login
- Password
- User
- Type (file,flash)
- PIN
- Action (request data login)

From this panel is possible to request the user to insert his data into a fake form.

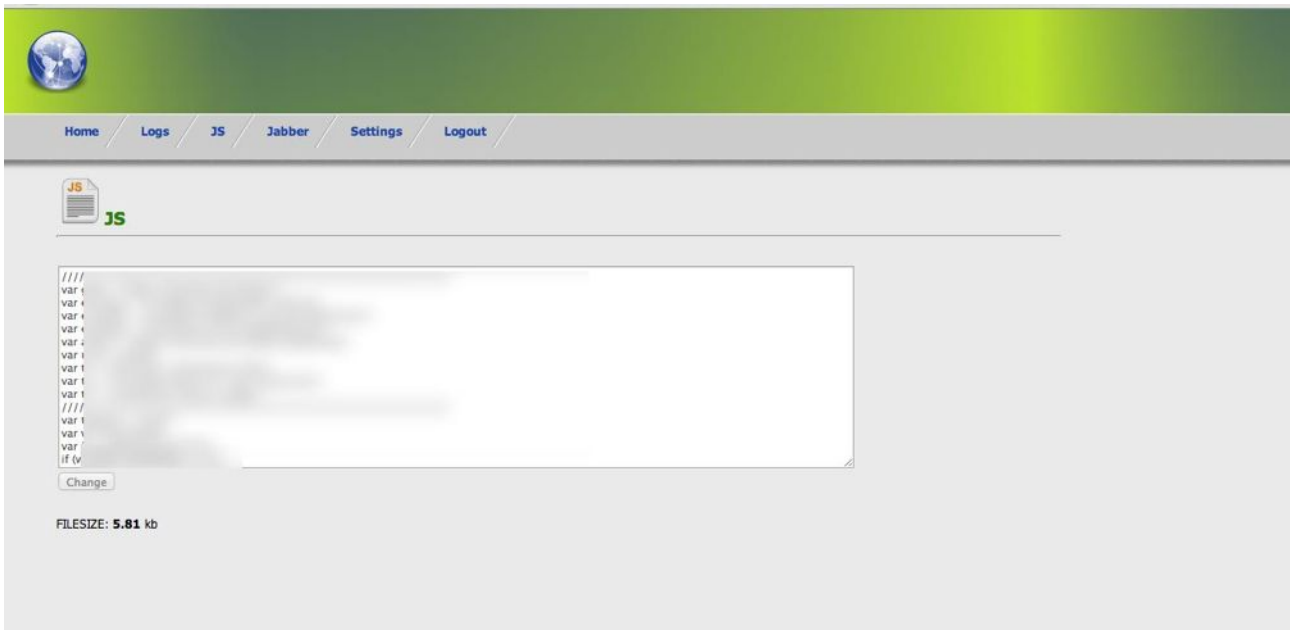


Clicking on the icons on the right is possible to send the request to some bot

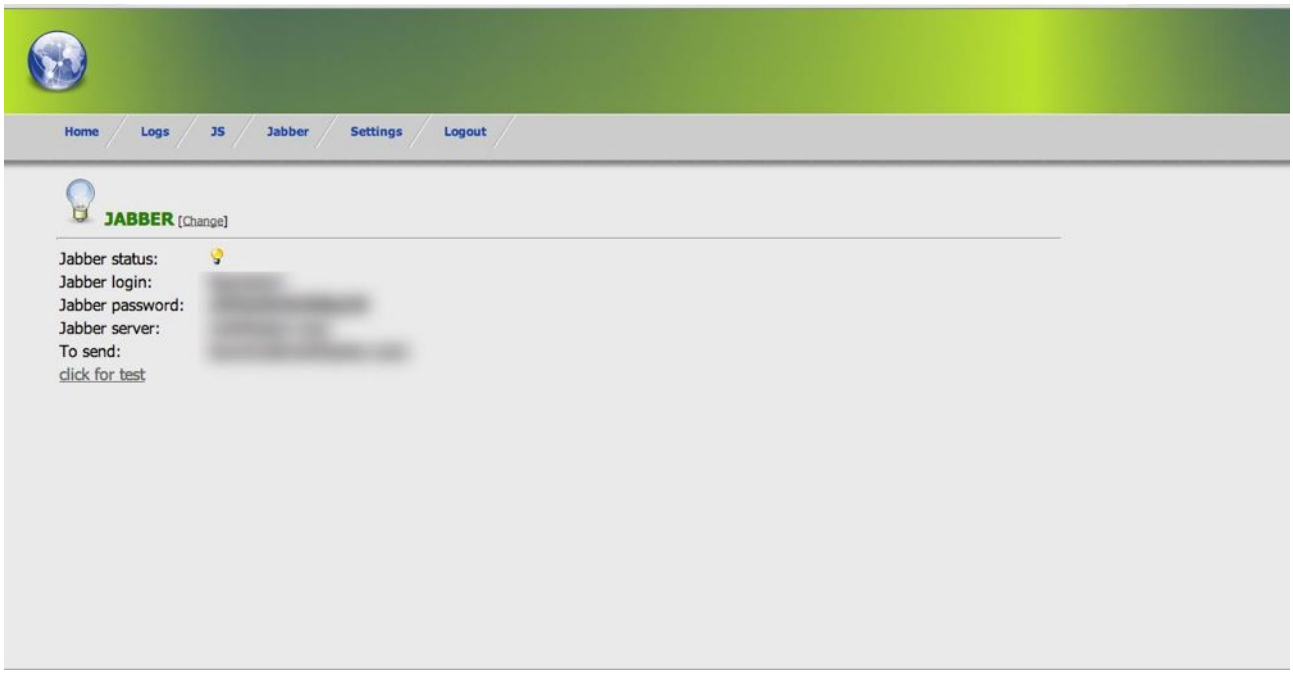


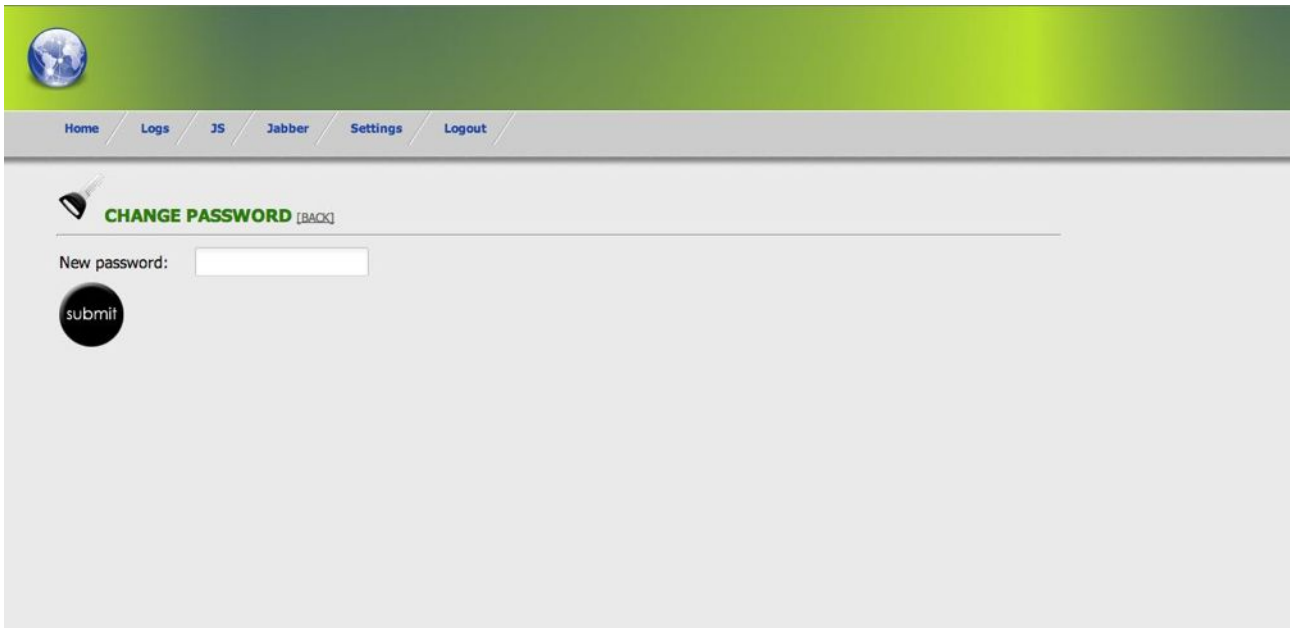
Analyzing every single bot is possible to see more details about it, clicking on the PIN.

The third page is the JS page, used by attacker to inject code inside the bot browser. To enable the form, there is a hidden command discovered through the JavaScript code analysis of that page.



The fourth section is the jabber page where an attacker can change his XMPP username and password and the last page is dedicated to set password for this panel.





CONCLUSION

The platform used by hacker is very powerful because is not only a drop-zone where data are sent, but is a real C&C server. They can interact with malware and can send it command to execute on the infected machine.

STATISTICS

The attack is alive and the amount of the hacked users is increasing every day, so until now we detect more than 40 hacked hosts and accounts.

ABOUT

Davide Cioccia

MSc Computer Engineering Degree. Security Developer focused on Cyber Security Intelligence, Malware analysis, Anti-fraud systems. Microsoft certified. Currently holding a Security Consultant position at Reply s.p.a - Communication Valley - Security Operations Center.

E-Mail: davide.cioccia@live.it

Twitter: https://twitter.com/david107

LinkedIn: https://www.linkedin.com/in/davidecioccia

Senad Aruch

Multiple Certified ISMS Professional with 10-year background in: IT Security, IDS and IPS, SIEM, SOC, Network Forensics, Malware Analyses, ISMS and RISK, Ethical Hacking, Vulnerability Management, Anti Fraud and Cyber Security.

E-Mail: senad.aruc@gmail.com

Blog: www.senadaruc.com

Twitter: https://twitter.com/senadaruch

LinkedIn: https://www.linkedin.com/in/senadaruc