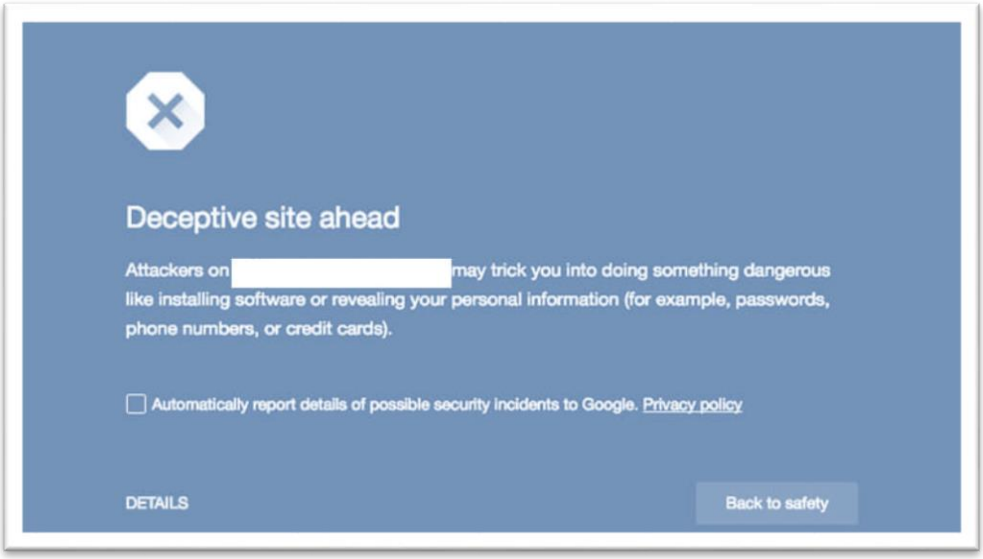
August
2017

The Economy Behind the Phishing Websites Creation



Deceptive site ahead

Attackers on [redacted] may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

□ Automatically report details of possible security incidents to Google. Privacy policy

ClearSky Cyber Security

Table of Contents

Summary

The main aim of this research is to understand and describe the eco-systems of fake websites developers and designers, and the basic economy behind creation of fake websites that impersonate legitimate websites of banks, credit cards companies and corporations. Mostly, the aim of those fake websites is stealing credential (banking or corporate) or credit cards information.

As part of this research we checked dozens of popular Russian and English-speaking underground boards and forums, looking for vendors' topics that provide services of fake webpages creation. On the second stage, when it was available, we conducted HUMINT operation and made a direct contact with those cybercrime vendors of fake sites via instant messaging (mostly jabber) to get deeper understanding of their skills, works and pricing.

Totally, we have checked about 15 different phishing vendors, when the main criteria were the skills of the vendor, the prices and how he makes the fake site.

We have checked a price for two main types of fake sites:

1. **Banking login page** that is similar to real one - when the aim is to steal the login and the password to banking account.
2. **Second stage to the banking login page** in order to steal additional information - page that do not exist in real bank website and asks the user to enter their credit cards number, expiration date and CVV number.

In addition, we have checked whether the vendors are just duplicating the original website, or developing it from scratch/partially.

Why does it matter? – Because mostly the duplicated websites are being exposed and taken down quicker, and as one vendors (Vendor9) told us – duplicated websites, in many cases are being blocked by Chrome/Safari:

> *Vendor9: it is foolish to duplicate – will be exposed immediately*
> *Vendor9: in chrome/safari*
> *Vendor9: I'm developing myself*

Some of the vendors (like *Vendor5*), also add some kinds of filters to prolong the time of the fake website till it is being exposed:

> *Vendor5: I have also another filter*
> *Vendor5: the life time is significantly longer*
> *ClearSky: which filter?*
> *Vendor5: as a defense from different bots*
> *Vendor5: and scanners*

We have seen that some of the vendors, mostly the more qualified ones are aware of those issues and mention it in the conversation, while the lower quality "developers", or in other words the script kiddies who try to earn money don't even understand what is the difference between just duplicate a website and develop a fake from scratch. To note, that some of the vendors, duplicate the website and make basic "cleaning" i.e. basic changes in HTML and content.

Below is a table that summarizes the key points of the research (to note that in the public version of this report we censored the nicknames of the vendors. This is done for the purpose of not promoting them):

Vendor	Abilities	Beginning of the service	Price for fake banking login	Price including another page for CC+EXP+CVV grabbing	Duplicate/ Develop
Vendor1	Back-End, Front-End developer – limited knowledge	January 2016	25 - 100 $	150 $	Duplicate
Vendor2	Developer with 5 years' experience	February 2017	15$	50$	Duplicate
Vendor3	Developer with Javascript, HTML, CSS, PHP, jQuery, Bootstrap, Sql, Sqlite knowledge	September 2015	150$	150	Duplicate
Vendor4	Designer and developer	November 2016	Begins on 100$		Develop
Vendor5	Developer	2015	200$	250$	Develop
Vendor6	Developer	May 2017	100$	150$	Depends on the complexity
Vendor7	Developer – limited knowledge	August 2016	30$	250$	Duplicate, for complex fakes - develop
Vendor8	Developer	May 2016	17-42$	-	Duplicate
Vendor9	PHP Developer	April 2017	40$ + feedback	100$	Develop
Vendor10	Developer	February 2017	70$	No additional charge	Develop
Vendor11	-	February 2017	~17$	-	Duplicate
Vendor12	-	May 2017	40$	65$	Develop
Vendor13	Front End Developer	June 2017	33$	50$	Develop
Vendor14	Basic knowledge in HTML and CSS	April 2017	50$	-	Develop

We can see that there are two different types of professionals who are required to fake websites creation: the **developers** and the **designers**. Some of the fake websites service providers, who are developers, work with 3rd party designers when a design / change in the websites is required. We can see it from our conversation with one of the vendors named "*Vendor2*":

> *Vendor2: there is separate design studio, we can separately make highly professional template*
> *Vendor2: regarding the design. He is a partner. He works officially.*
> *Vendor2: I build shops, make up mails, fakes. Can conduct projects .Design I even don't offer, will talk with him regarding his works*

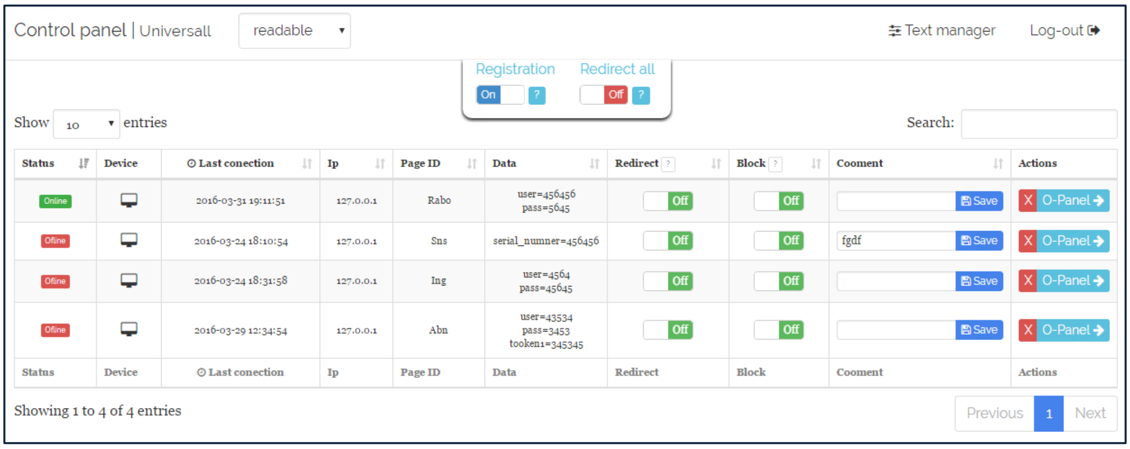
From pricing point of view, **the average price for banking login page is about 60$**, when the pricing is mostly divided into two groups, those who just duplicate the original site mostly price it at about 20-30$ and those who develop the fake website from scratch price it at 50$ or more, when some of the vendors ask about 150-200$ for their work.

When we asked for **pricing for additional page that not exist at real websites, for grabbing and stealing credit cards data, in some cases the price was significantly raised** because this additional page required some development and design work, and not just duplicating existing page.

Some of the fake sites vendors, also develop different tools and panels that allow them to collect in a proper and comfortable way the stolen credentials and offering it for additional payment to fake websites buyers.

One of the additional services that some vendors offer is control panels that allow collecting all the required data and log in convenient manner.

One panel is introduced and beign sold by *"Vendor3"*:



Show 10 entries

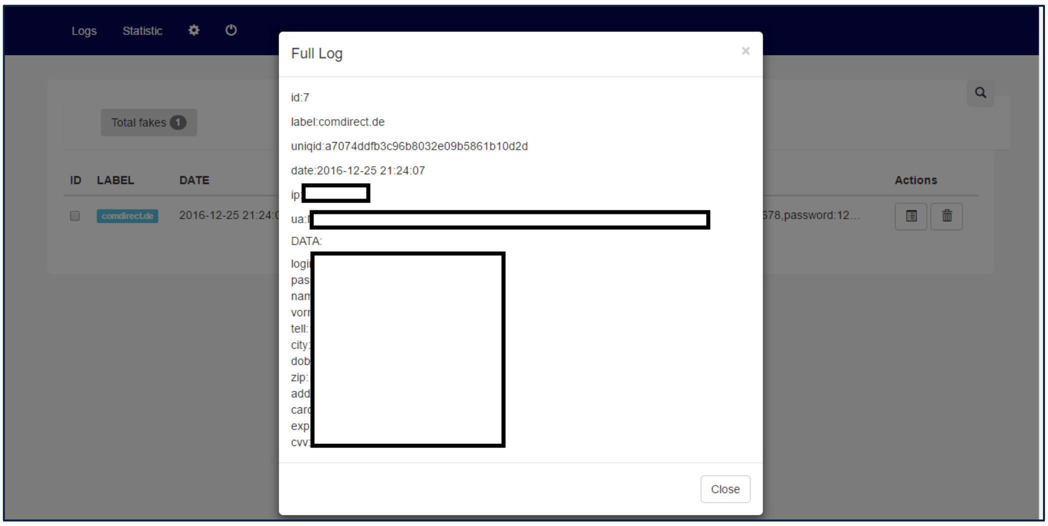
Search:

Status	Device	Last conection	Ip	Page ID	Data	Redirect ?	Block ?	Cooment	Actions
Online	🖥	2016-03-31 19:11:51	127.0.0.1	Rabo	user=456456 pass=5645	Off	Off	Save	X O-Panel
Ofline	🖥	2016-03-24 18:10:54	127.0.0.1	Sns	serial_numner=456456	Off	Off	fgdf Save	X O-Panel
Ofline	🖥	2016-03-24 18:31:58	127.0.0.1	Ing	user=4564 pass=45645	Off	Off	Save	X O-Panel
Ofline	🖥	2016-03-29 12:34:54	127.0.0.1	Abn	user=43534 pass=3453 tooken1=345345	Off	Off	Save	X O-Panel
Status	Device	Last conection	Ip	Page ID	Data	Redirect	Block	Cooment	Actions

Showing 1 to 4 of 4 entries

Previous 1 Next

Another one is built and developed by *"Vendor5"*:



id:7

label:comdirect.de

uniqid:a7074ddfb3c96b8032e09b5861b10d2d

date:2016-12-25 21:24:07

ip:[redacted]

ua:[redacted]

DATA:

logi
pas
nam
vor
tell:
city:
dob
zip:
add
car
exp
cvv
[redacted]

Most of the vendors, work very hard to promote their services, constantly pump up their topics in different forums, and although the basic pricing of most of them is relatively low, in order to gain proper reputation, they offer various kinds of actions and discount.

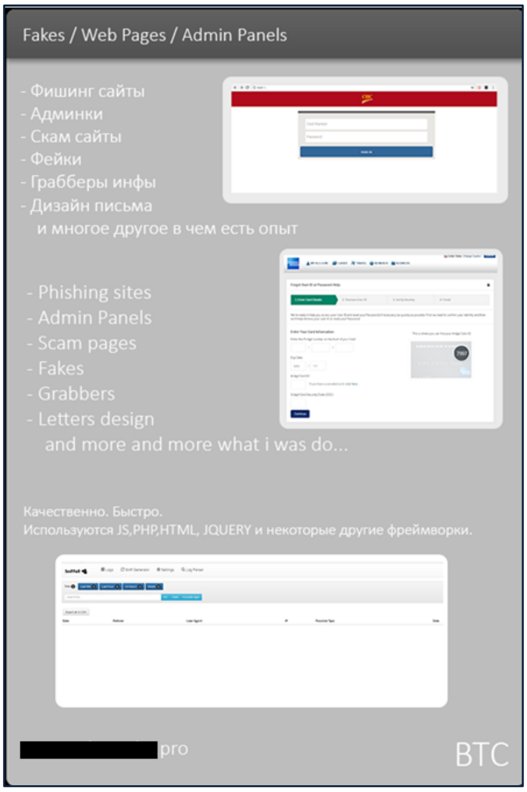
For example, one of the young leading vendors of the last year, *"Vendor1"*, offered free creation of fake websites for TLD .de for limited time:

> *Hello to Everyone!*
> *Brother Bear provides free service that is available only till 9th May.*
> *Creation of fake websites to not very important services from TLD DE – for free.)*
> *To one person from the forum – 1 fake.)*
> *Write via the contacts and after receiving the result – post here your feedback.)*
> *Thanks all for the attention.*
> *p.s. Regards Vendor1*

This quotation, as well as most of the quotations, and conversations with the vendors, was originally in Russian, and were translated, edited and redacted when it was necessary, while we tried to keep the essence of the chat and the language level as near to the original as it was possible.

In terms of time, there are vendors who are ready to conduct their work in timeframe of ten minutes or within an hour, but there are vendors who ask for several days.

Some of the vendors also publish colorful advertisements:



Fakes / Web Pages / Admin Panels

- Фишинг сайты
- Админки
- Скам сайты
- Фейки
- Грабберы инфы
- Дизайн письма

и многое другое в чем есть опыт

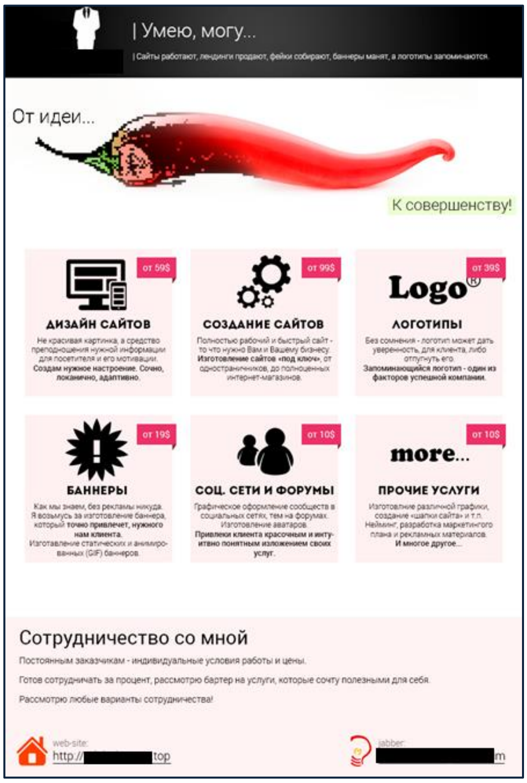
- Phishing sites
- Admin Panels
- Scam pages
- Fakes
- Grabbers
- Letters design

and more and more what i was do...

Качественно. Быстро.
Используются JS,PHP,HTML, JQUERY и некоторые другие фреймворки.

[redacted]pro

BTC



[redacted]

| Умею, могу...

| Сайты работают, лендинги продают, фейки собирают, баннеры манят, а логотипы запоминаются.

от 59$
ДИЗАЙН САЙТОВ
Не красивая картинка, а средство преподношения нужной информации для посетителя и его мотивации. **Создам нужное настроение. Сочно, локанично, адаптивно.**

от 99$
СОЗДАНИЕ САЙТОВ
Полностью рабочий и быстрый сайт - то что нужно Вам и Вашему бизнесу. **Изготовление сайтов «под ключ»**, от одностраничников, до полноценных интернет-магазинов.

от 39$
ЛОГОТИПЫ
Без сомнения - логотип может дать уверенность, для клиента, либо отпугнуть его. **Запоминающийся логотип - один из факторов успешной компании.**

от 19$
БАННЕРЫ
Как мы знаем, без рекламы никуда. Я возьмусь за изготовление баннера, который **точно привлечет, нужного нам клиента.** Изготавление статических и анимированных (GIF) баннеров.

от 10$
СОЦ. СЕТИ И ФОРУМЫ
Графическое оформление сообществ в социальных сетях, тем на форумах. Изготовление аватаров. **Привлеки клиента красочным и интуитвно понятным изложением своих услуг.**

от 10$
ПРОЧИЕ УСЛУГИ
Изготовлние различной графики, создание «шапки сайта» и т.п. Нейминг, разработка маркетингого плана и рекламных материалов. **И многое другое...**

Сотрудничество со мной

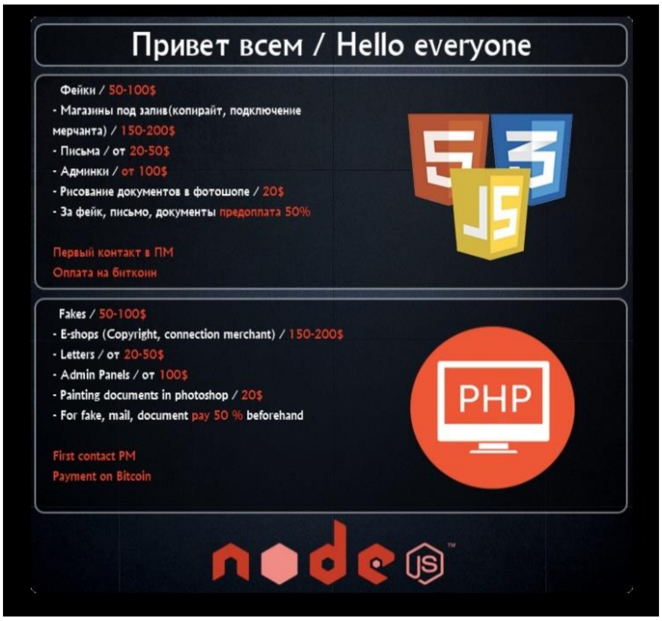
Постоянным заказчикам - индивидуальные условия работы и цены.

Готов сотрудничать за процент, рассмотрю бартер на услуги, которые сочту полезными для себя.

Рассмотрю любые варианты сотрудничества!

web-site:
http://[redacted]top

jabber:
[redacted]m



Привет всем / Hello everyone

Фейки / 50-100$
- Магазины под залив(копирайт, подключение мерчанта) / 150-200$
- Письма / от 20-50$
- Админки / от 100$
- Рисование документов в фотошопе / 20$
- За фейк, письмо, документы предоплата 50%

Первый контакт в ПМ
Оплата на биткоин

Fakes / 50-100$
- E-shops (Copyright, connection merchant) / 150-200$
- Letters / от 20-50$
- Admin Panels / от 100$
- Painting documents in photoshop / 20$
- For fake, mail, document pay 50 % beforehand

First contact PM
Payment on Bitcoin

As they are acting as service providers, most of the vendors are very polity and patient to answer any questions that potential clients have (even too polite):

> *Vendor1: Thank you very much.) Good evening to you also. Write in any convenient time to you, i'm always available. Will do everything quickly and with high quality.*

One of the vendors we had a conversation with, mentioned also some interesting points about creating good banking fakes:

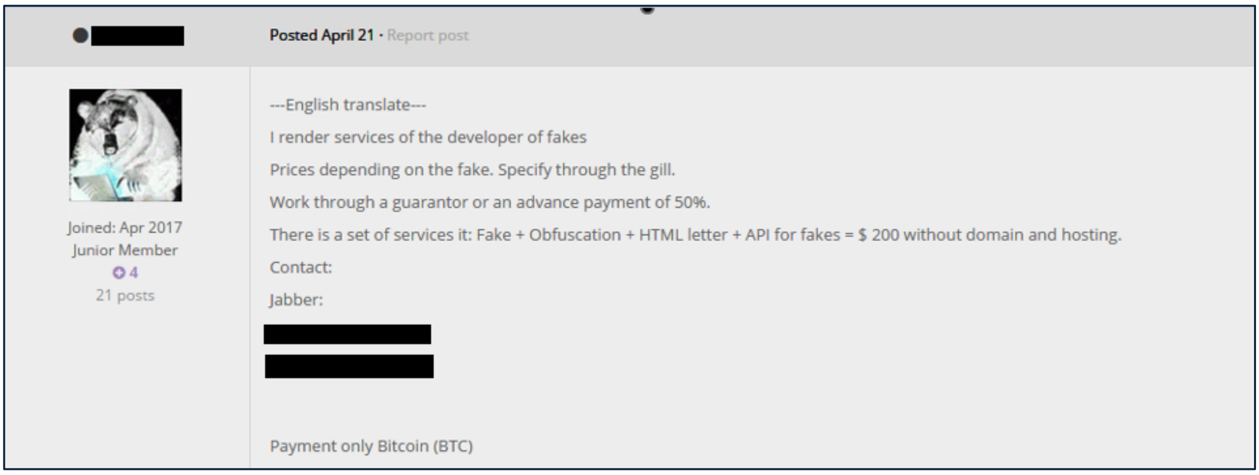
> *Vendor4: I did such fakes for landing for CC grabbing, something else. Landings for (malicious – Clearsky) downloads, mostly fakes for corp. websites (duplicates or based on the original) for scamming.*
>
> *ClearSky: shortly, everything except for banks*
>
> *Vendor4: except for banks/retail/ social networks)*
>
> *…*
>
> *Vendor4: why I don't like fakes. If it is required just to make logs of the data from the forms (to txt or to mail) – welcome, I can do it. If it is required to do validation of the credentials on the original server, it is not for me. Better talk with those who specialize on this) will be done faster and will cost less) I simply don't have time to deal with this. Understand me.*
>
> *Vendor4: things that I'm proficient in, I do good and properly, what I'm not – and don't have time to study (because of high amount of work), so better I'll refuse than not keeping the deadline and losing my reputation.*

In this research, we present in depth the vendors, their modus operandi and pricing and examples of their previously done works.

Actors

Vendor1

The first vendor, *"Vendor1"*, offers fake websites developments services, beginning from January 2016. He is mostly active in Russian speaking forums, but also tries to advertise his services in English speaking boards, although it is visible that he is not proficient in English:



● [redacted]

Posted April 21 · Report post

Joined: Apr 2017
Junior Member
4
21 posts

---English translate---

I render services of the developer of fakes

Prices depending on the fake. Specify through the gill.

Work through a guarantor or an advance payment of 50%.

There is a set of services it: Fake + Obfuscation + HTML letter + API for fakes = $ 200 without domain and hosting.

Contact:

Jabber:

[redacted]

Payment only Bitcoin (BTC)

From this post, we can see one of his pricing offers - providing a full set of services for someone who conducts phishing activity, this includes: fake website + obfuscation + HTML mail + API (for credential grabbing) for 200$, not including the domain registration and the hosting. In other post, he explains that he has "API for fakes" that allows to gather credential stolen from different fake websites to one admin panel on another hosting. This offer is higher than average pricing, and as to our assessment it is possible to bargain the price.

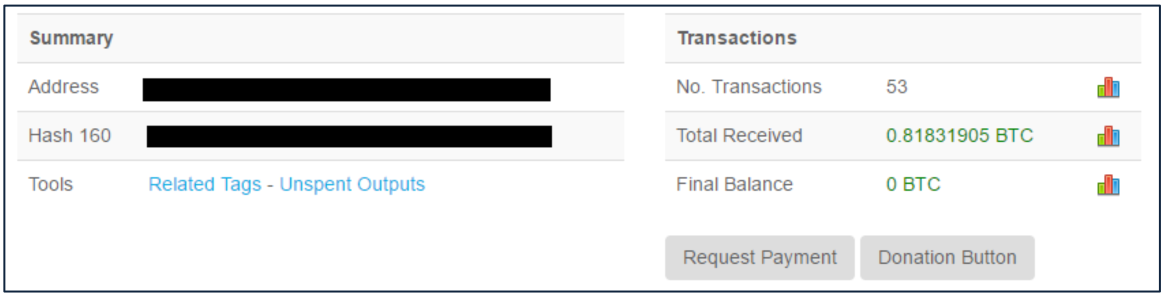
Checking his history and posts on other boards, we see that he defines himself as back-end and front-end web developer but not as designer/ painter. At some stage of the work, in April 2017, he updated that his team has additional front-end developer, so he can conduct the orders even quicker.

Although, he advertises his services also in English speaking forums, lately, in May he posted that he is not ready to work with English speaking persons, especially those who want to create fake pages to Russian entities (e.g Sberbank):

> *I don't work with all the English-speaking representatives of the manhood! No way! In no circumstances!*
> *Especially with those who write "You can make scam page sberbank + curl validation script?"*
> *I will immediately write here, in the forum about such "Heroes" that work on RU.*
> *Thank you that you read and acknowledged with this message.*
> *If you are "I no understand russian", etc. – those are not my problems in any way.*
> *There is google translate – so use it!*
> *For everyone else – only good: I'm free for now from orders.*
> *P.S. Best Regards Vendor1*

He works via escrow or 50% pre-payment only; via BTC and the results are provided in some cases immediately.

One of his payment wallets was exposed and by checking it we can see many of the professional activity of this vendor in the end of 2016 - beginning of 2017:



Summary	
Address	[redacted]
Hash 160	[redacted]
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	53
Total Received	0.81831905 BTC
Final Balance	0 BTC

Below are the incoming transactions details, that allows us to understand about the income of phishing pages vendor:

Date	BTC	$ (in the time of the transaction)
2016-11-20	0.00670527 BTC	4.97
2016-11-26	0.00685868 BTC	5.01
2016-12-19	0.01897575 BTC	15
2016-12-20	0.0189285 BTC	15
2016-12-29	0.0103088 BTC	9.97
2016-12-30	0.0104249 BTC	10.01
2017-01-15	0.0245922 BTC	20.04
2017-01-16	0.0361335 BTC	30
2017-01-19	0.055144 BTC	49.99
2017-01-23	0.0543085 BTC	50.03
2017-01-23	0.027001 BTC	25.03
2017-01-23	0.05393743 BTC	49.97
2017-01-26	0.05500671 BTC	50.44
2017-01-27	0.021888 BTC	20.12
2017-01-31	0.036708	34.96
2017-01-31	0.036771 BTC	35.01
2017-02-06	0.014994 BTC	15.25
2017-02-07	0.02408 BTC	25.36
2017-02-08	0.024126 BTC	25.16
2017-02-08	0.03325921 BTC	35.19
2017-02-14	0.049371 BTC	49.87
2017-02-15	0.05 BTC	50.43
2017-02-15	0.014817 BTC	15
2017-02-18	0.02 BTC	21.09
2017-02-18	0.015 BTC	15.88
2017-02-19	0.08 BTC	84.48
2017-02-19	0.0189796 BTC	19.97

During those 3 months, the total income is about 800$, but the average income for each fishing website conducted (with a highly possible assumption that his only income is from fakes) – is really low, about 29$.

This transaction report from Blockchain is going together with his basic pricing that is very low. Basic fake website that requires to put in the login + password and afterwards shows a message that required input of CC + expiration date + CVV – is 25$.

In one of the forums, he began offering his services during 2016 to make fake website for 300- 500 rubles (5-9 $). Because of his low prices, he needs to get a lot of clients, to profit. Therefor he also conducts different promotion actions, as well as discounts.

In beginning of May 2017, he launched a promotion for creating fake sites for Germany websites for free:

> *Hello to Everyone!*
> *Brother Bear provides free service that is available only till 9th May.*
> *Creation of fake websites to not very important services from TLD DE – for free.)*
> *To one person from the forum – 1 fake.)*
> *Write via the contacts and after receiving the result – post here your feedback.)*
> *Thanks all for the attention.*
> *p.s. Regards Vendor1*

This promotion run only one day, and was changed in a day for promotion with 20% discount:

> *Hello to Everyone!*
> *Bear launched yesterday small promotion and everyone who contacted me via jabber – received his free fakes.)*
> *Now is starting the second step of the promotion.) Following is the essence of this step.)*
> *I provide discount of 20% for all TLD's, except of RU (for Poland the discount is 30%)*
> *If the TLD is DE, and you order 1 fake, the second one is totally free.)) Any.)) Even for banking.))*
> *Thanks all for the attention if you read it.)*
> *p.s. Regards Vendor1*

As part of our investigation we conducted direct conversation with the vendor, and as part of it we understood his pricing that is between 50 to 100$ for fake (as to our understanding with possibility to bargain)

Below are the main parts of the conversation (edited and translated from Russian original)**:**

> *ClearSky: I want to know the pricing for a relatively simple fake*
>
> *Vendor1: Starting from 50$*
> *Vendor1: Anything do to with CC, starts from 100$*
>
> *ClearSky: that's a reasonable base price …what is the maximum?*
> *ClearSky: what will add to the cost?*
>
> *Vendor1: The complication and the type of the website*
>
> *ClearSky: for example, the website online.***bank.** (redacted by Clearsky)*
>
> *Vendor1: Do you need desktop and mobile version?*
>
> *ClearSky: yes*
> *ClearSky: what is the difference in the price?*
>
> *Vendor1: exactly 100$.*
> *Vendor1: You are interested in a login page, am I right?*
>
> *ClearSky: yes*
>
> *Vendor1: So exactly 100$. Suits you?*
>
> *ClearSky: are you duplicating or developing?*
>
> *Vendor1: What is required?)*
>
> *ClearSky: duplicates get exposed faster*
>
> *Vendor1: Not necessarily my friend.) If it is duplicated – cleaning - obfuscation.)*
> *Vendor1: It will be like developed*
> *Vendor1: It only requires a couple of decent hands and some common sense*
>
> *….*

….

ClearSky: and if I also want to add to the fake another page (second stage) for cc + cvv … how will this affect the price?
ClearSky: this page doesn't exist on the real website

Vendor1: I can use the login page as a template and just add to it other fields
Vendor1: It won't add much, about +50$ considering the fact that it will be also obfuscated
Vendor1: And it is going without saying that there is support of all my works.

…

Vendor1: Understood. If the price is a bit too steep, there is room to bargain
Vendor1: People? A lot of people order banks pages with gathering of the info.

We succeeded to get logs from several of his conversation with his real customers, and those conversations provides us with deep understanding of fakes creation deals (all the conversations are originally in Russian).

From Vendor1 conversation with Customer 1 we can see the final low costs of fake works, about 25$ for a fake creation:

Vendor1: I hear you.

Customer1: https://,,,,,,?ei=mv_log-on
Customer1: need to collect login password
Customer1: after this to show a message that it is required to enter cc, expiration and cvv
Customer1: what will be the cost?

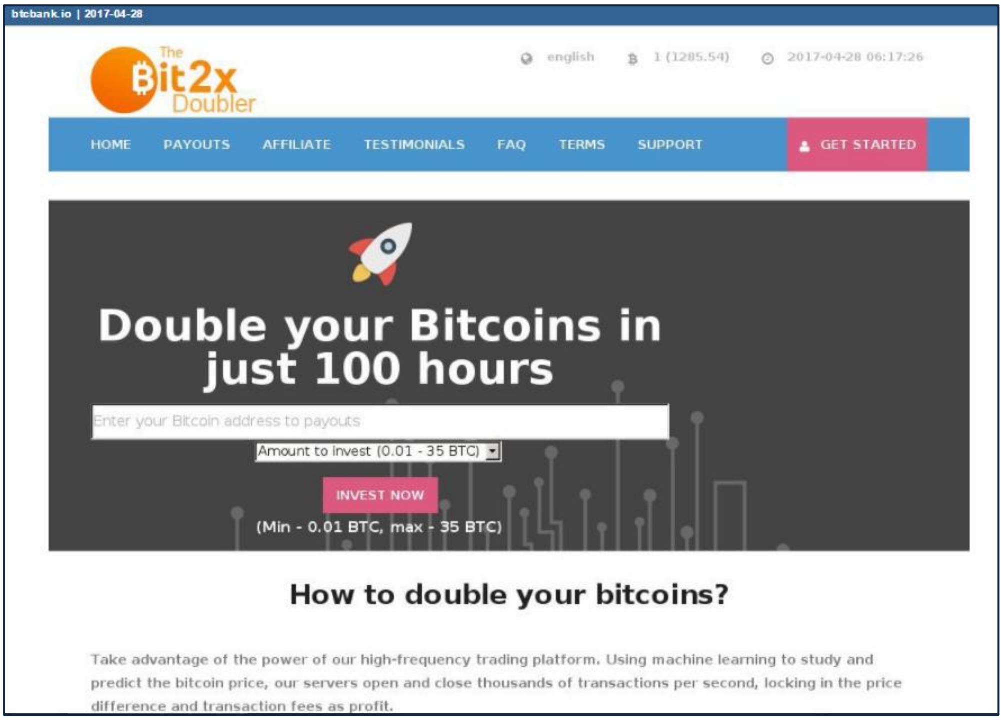
Vendor1 : 25 $

Customer1: do the fake, upload it to your hosting, I will test it– and if everything ok I pay 30

Vendor1: Pre pay 50% and I begin to work

Another conversation that was exposed is with another customer (Customer 2) that asked duplication of a website, changing the language of the website and adding to the payment page different BTC wallet. All this is only about 30$. From this conversation, we can see also that these fakes vendor abilities are very limited.

The website that was ordered to be duplicated is btcbank.io:



btcbank.io | 2017-04-28

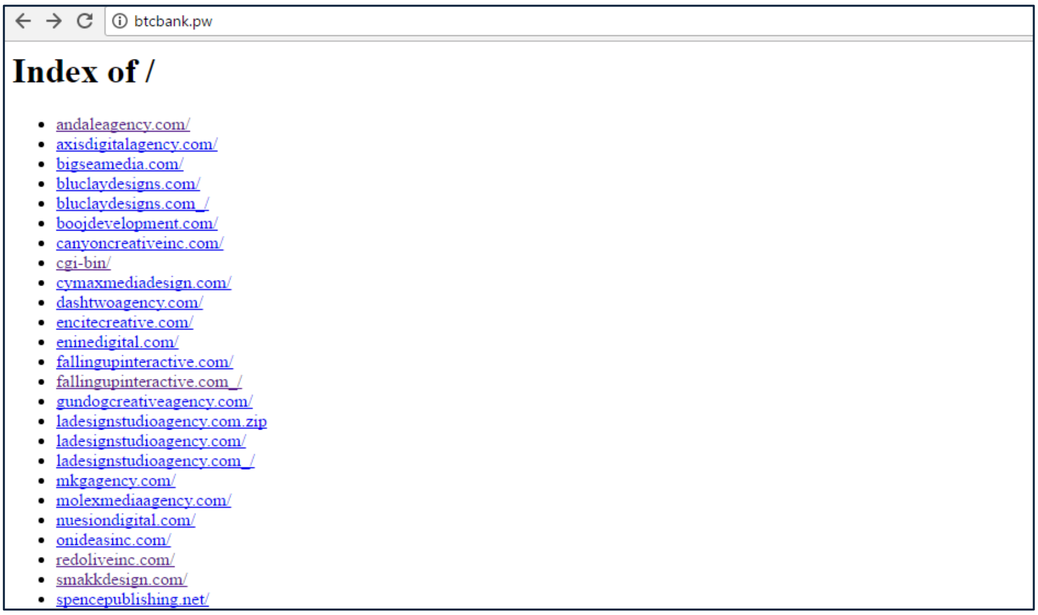
Double your Bitcoins in just 100 hours

(Min - 0.01 BTC, max - 35 BTC)

How to double your bitcoins?

Take advantage of the power of our high-frequency trading platform. Using machine learning to study and predict the bitcoin price, our servers open and close thousands of transactions per second, locking in the price difference and transaction fees as profit.

The fake domain name that was opened to this affair is btcbank[.]pw, btcbank[.]win and bitcoindoubler2017[.]com. In the websites themselves we see mostly hosted different websites that impersonating web design and advertisement agencies:

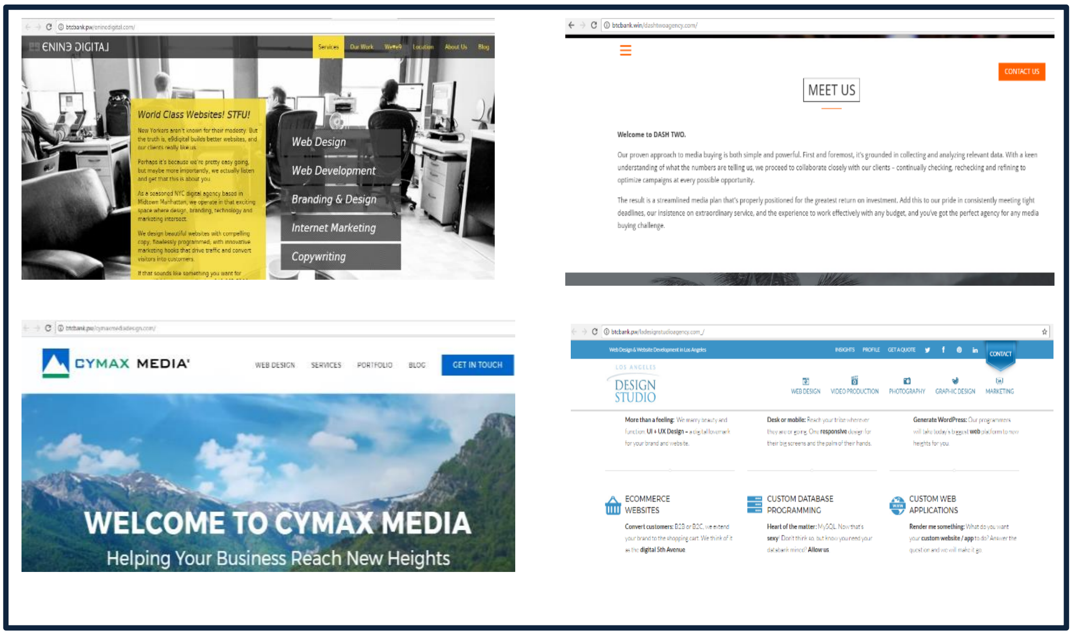


btcbank.pw

Index of /

- andaleagency.com/
- axisdigitalagency.com/
- bigseamedia.com/
- bluclaydesigns.com/
- bluclaydesigns.com_/
- boojdevelopment.com/
- canyoncreativeinc.com/
- cgi-bin/
- cymaxmediadesign.com/
- dashtwoagency.com/
- encitecreative.com/
- eninedigital.com/
- fallingupinteractive.com/
- fallingupinteractive.com_/
- gundogcreativeagency.com/
- ladesignstudioagency.com.zip
- ladesignstudioagency.com/
- ladesignstudioagency.com_/
- mkgagency.com/
- molexmediaagency.com/
- nuesiondigital.com/
- onideasinc.com/
- redoliveinc.com/
- smakkdesign.com/
- spencepublishing.net/

Below are samples of several of the fake website hosted on the server and impersonating real organizations:



Below are relevant excerpts from the conversation between *"Vendor1"* and *"Customer 2"*:

CUSTOMER 2: for example, I need to duplicate the site btcbank.io, to change the language and to add to the payment page my btc wallet + to connect exchanger. Can you do such a thing?
…
…
Vendor1: See, to make a fake of the website and to change the language – it is not expensive
CUSTOMER 2: html…http
Vendor1: 30$ dollars *Vendor1: It is pure HTML, CSS, JS. If you want to connect exchanger – it will cost more*

CUSTOMER 2: but you are able to do this?

CUSTOMER 2: the question is whether you are able or not

CUSTOMER 2: I need this type of work all the time

…

CUSTOMER 2: it seems that what I need is to copy the website, to replace the text. I will prepare the text, and will give it to you. I need to be able to upload to my domains the content, and that's all

CUSTOMER 2: superb

CUSTOMER 2: good evening

Vendor1: Thank you very much.) Good evening to you also. Write in any convenient time to you, i'm always available. Will do everything quickly and with high quality.

…

…

CUSTOMER 2: so, I'm ready to order. Need full copy of the website btcbank.io

Vendor1: And in the home page should be your wallet, that it will look like you are the last who paid.

Vendor1: Right?

CUSTOMER 2: I don't understand

Vendor1: btcbank.io

Vendor1: In the page where there is a list of wallets that deposited money

CUSTOMER 2: oh, yes

CUSTOMER 2: there should be my wallet. right. and I must have the possibility to edit it, simply say me where

…

…

Vendor1: See it, I can't duplicate the chat window, it is part of site's engine

Vendor1: The red window that is in the top, I will try to add also

…

Vendor1: In the terms of time – I need for this 5 days.

...

Vendor1: I have someone who can do such a work. He is already sleeping, but I will contact him tomorrow and solve the issue

CUSTOMER 2: a normal person?

Vendor1: Yes. We know each other for a long time and he doesn't bullshit me.

CUSTOMER 2: you yourself don't change – design the templates?

Vendor1: I'm Back-End, Front-End , and that's all. I'm a painter like Hitler is Mother Teresa.

…

…

CUSTOMER 2: how much should I pay for the logo and your work?

Vendor1: The remaining 50% is 10$, for the chat – pay the sum you ready to pay and for the logo 10$.

CUSTOMER 2: I sent 30

CUSTOMER 2: bonus for quick work

Another conversation of this vendor shows the process (and the low payment of about 20$) for fake page for cartetitolari.mps.it, Italian credit cards service:

Customer 3: regarding fakes
Customer 3: do you make?

Vendor1: I do.

Customer 3: https://www.cartetitolari.mps.it/
Customer 3: what will be the price?

Vendor1: 20$

Customer 3: can you show examples?

Vendor1: no problem.
*Vendor1: https://****.ws/threads/fejk-blockchain-inf****

….

….

Customer 3: I will tell what info to grab after the login?
Customer 3: need to grab info
Customer 3: I'm sending you 10$ for now

Vendor1: There on the page place to enter login and password, so only this info can be grabbed
Vendor1: ok.

Customer 3: I know, but it can be not enough

Vendor1: I'm listening to your requests.

Customer 3: as always. Do you do obfuscation?
Customer 3: sending to mail?
Customer 3: if you don't do obfuscation, I will order from someone else

Vendor1: Sending to mail or reports by logs, will be to ftp.

Customer 3: I need it to be sent. Can you?
Customer 3: ok ok, ftp is ok

Vendor1: obfuscation I don't do. Sending to mail can do.

….

….

Customer 3: the logs are sent to ftp, yes,

Vendor1: they are being saved on ftp.
Vendor1: the same ftp that hosts this site

Customer 3: in short, locally
Customer 3: not in ftp

….

Customer 3: where it is saved?

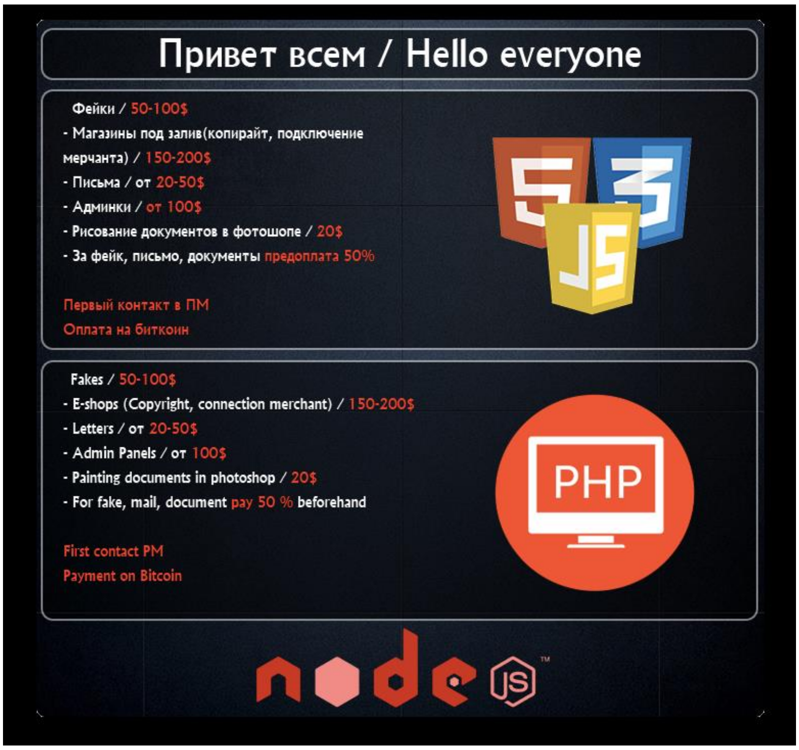
Vendor1: into data_cc.txt

Vendor2

Another vendor who is offering web sites/ fakes development services is *"Vendor2"* posted the following topic in one of the underground forums in February 2017:

> *Web development /Creation of websites of any difficulty":*
> *Services:*
> *1) Creating a website (any difficulty).*
> *Working with php, phyton, javascript, SQL.*
> *Engines: Drupal, Wordpress, Opencart, yii2, django*
> *2) Imposition of any pattern of difficulty*
> *3) Make-up for mobile devices*
> *4) Develop a site design, emal letter panache banners, logos*
> *5) Site Promotion - social networks, instagramm, Google, Yandex*
> *6) Remaking documents in Photoshop*
>
> *Advance payment 50%.*
> *Contact details:*
> *Jabber: (redacted)*
>
> *If necessary, I can put together a team*
>
> *Payment on Bitcoin or webmoney*

But this topic didn't work well for him and didn't attract potential clients, so in May 16th he launched a new topic advertising his services, this time with colorful graphical advertisement and basic pricing :



Привет всем / Hello everyone

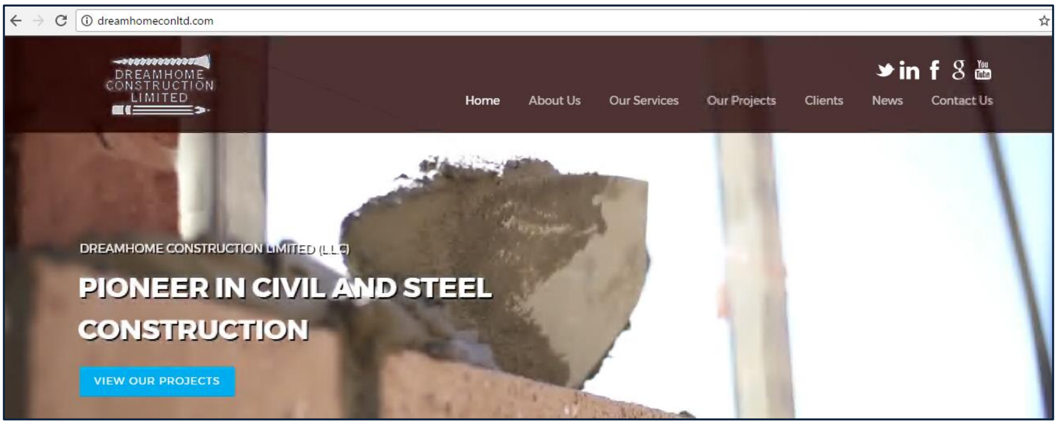
Фейки / 50-100$
- Магазины под залив(копирайт, подключение мерчанта) / 150-200$
- Письма / от 20-50$
- Админки / от 100$
- Рисование документов в фотошопе / 20$
- За фейк, письмо, документы предоплата 50%

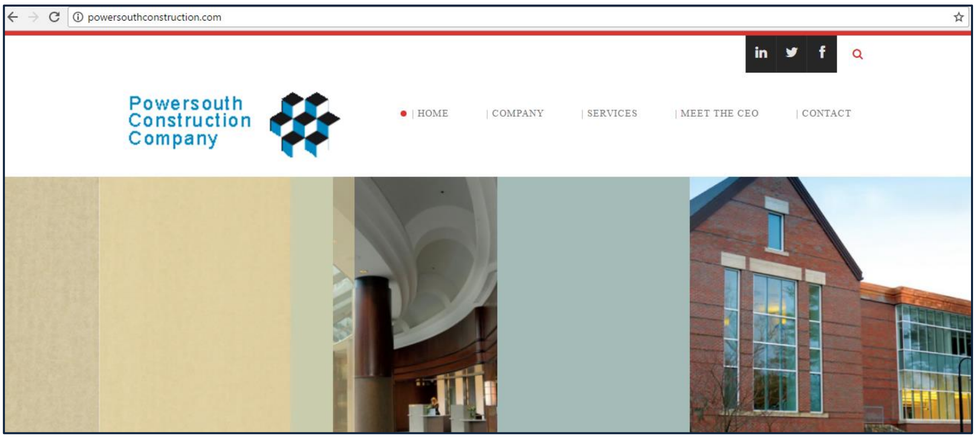
Первый контакт в ПМ
Оплата на биткоин

Fakes / 50-100$
- E-shops (Copyright, connection merchant) / 150-200$
- Letters / от 20-50$
- Admin Panels / от 100$
- Painting documents in photoshop / 20$
- For fake, mail, document pay 50 % beforehand

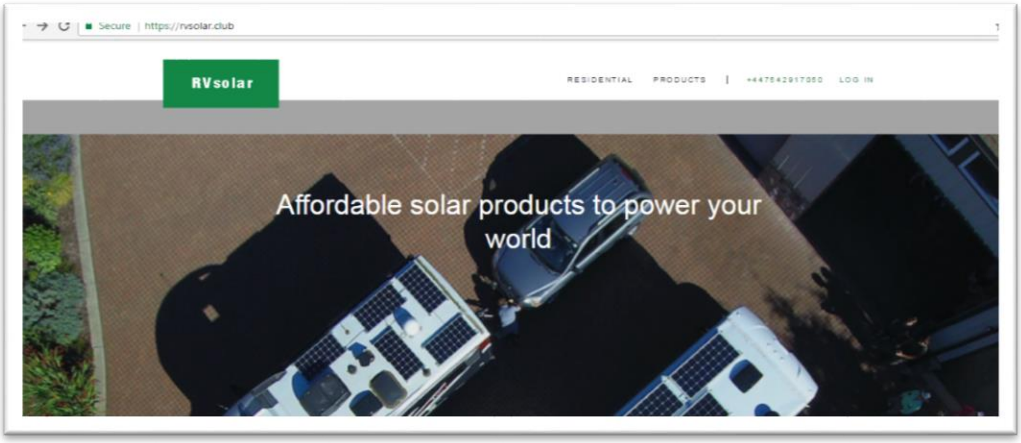
First contact PM
Payment on Bitcoin

As part of our direct contact with the vendor we have seen that his pricing for basic banking fakes is very low and begins as low as 15$ for duplicating the required page. If it required to develop and design a new page or website, the **vendor works with separate design studio**, that is a legitimate studio that basically provide normal design services. He has 5 years' experience, and provided 2 examples of fake websites he done lately


dreamhomeconltd.com
DREAMHOME CONSTRUCTION LIMITED
Home
About Us
Our Services
Our Projects
Clients
News
Contact Us
DREAMHOME CONSTRUCTION LIMITED (LLC)
PIONEER IN CIVIL AND STEEL CONSTRUCTION
VIEW OUR PROJECTS



As well he has provided an example for a shop he developed, that its aim is money laundering:



Below is our full conversation with this vendor:

ClearSky: I'm regarding the fakes

Vendor2: hi now I received a work. I can begin tomorrow. What fake do you need?

ClearSky: fake of banking login
*ClearSky: like online.***.co.***
ClearSky: what is the pricing?

Vendor2 solely for this page is 15$

ClearSky: are you duplicating or developing?

Vendor2: duplicating

Vendor2: what does it mean developing? to do something in photoshop?

Vendor2: there is separate design studio, we can separately make highly professional template

ClearSky: and what will be the price for a template of such a website? Or if I will add additional page that doesn't exist in the original?

...

ClearSky: good day, do you have an answer?

Vendor2: yes, I have. It is not cheap 3000 rubles

Vendor2: for one page

ClearSky: understand. Not cheap.

ClearSky: do you have examples of works? Or feedback?

Vendor2: regarding the design. It is a partner. He works officially.

Vendor2: I build shops, make up mails, fakes. Can conduct projects .Design I even don't offer, will talk with him regarding his works.

ClearSky: understand. And examples/ feedbacks of your works?

Vendor2: powersouthconstruction[.]com ,   http://dreamhomeconltd[.]com

Vendor2: recent fakes

Vendor2: generally I collected a lot of projects

Vendor2: experience of 5 years

Vendor2: here in (redacted – Clearsky) I am a new member

ClearSky: ok. Thx.

…

…

Vendor2: http://rvsolar[.]club

Vendor2: shop for money laundering

Vendor3

This vendor began his offering in September 2015 which included variety of services like Android and Windows injections for different bots, **Phishing Pages and Fakes, and Phishing Pages with SMS/Token intercept.**

The vendor presents himself as someone who is proficient in JavaScript, HTML, CSS, PHP, jQuery, Bootstrap, SQL and SQLite.

In direct conversation with the vendor we have seen that a price for basic banking login fake that is suitable for desktop and mobile costs 150$, **including the ability to add additional pages for stealing credit cards information**. To be noted - he is not developing the pages from scratch, but duplicating the pages with slight changes in HTML elements and texts.

This vendor biggest specialty is phishing pages with SMS/Token intercept (mostly android injections), allows to bypass the defenses that use One Time Password (OTP token), using mechanism that allows the malicious attacker to use this token during 30 second, before the next page is loaded in victim's machine.

During last June, the vendor posted an explanation what he does to protect his fake page against detection, and mentioned several issues:

1. HTML Encode - all body content of the page looks incomprehensible, building it by JavaScript document.write function (for clients it don't make any difficulties to edit code because all this encoding been made by PHP while page render)
2. Although, he doesn't develop the pages from scratch, he recommends conducting the following changes to keep the pages undetected:
   a. Keep all files locally
   b. Scale and rename all images
   c. Filter all text content with special tools
3. Generating unique URL for every visitor
4. Browser notifications – using several tricks to gets rid of all browser notifications for all his pages.

Clearsky: I want to know the pricing for relatively simple fake

*Clearsky: like online. ***bank.co.***

Vendor3: it is not simple

Vendor3: fake desk. + mobile = 150$

Vendor3: what more can I help in?

Clearsky: and if I add to the fake another page (second stage) for (collecting -Clearsky) cc + cvv … how it changes the price?

Vendor3: the same price

Clearsky: ok

Vendor3: see

Vendor3: you order a fake

Vendor3: and you will have a week

Vendor3: to decide about stages

Vendor3: and parameters

Vendor3: of course, there are limits to everything

Vendor3: but to add one stage ore one parameter is not a problem

Vendor3: it doesn't influence the price

Clearsky: are you duplicating or developing from scratch?

Vendor3: what's the difference?

Clearsky: in some cases, the duplicated are being exposed quicker

Vendor3: I change elements in HTML

Vendor3: it is the same as to developed

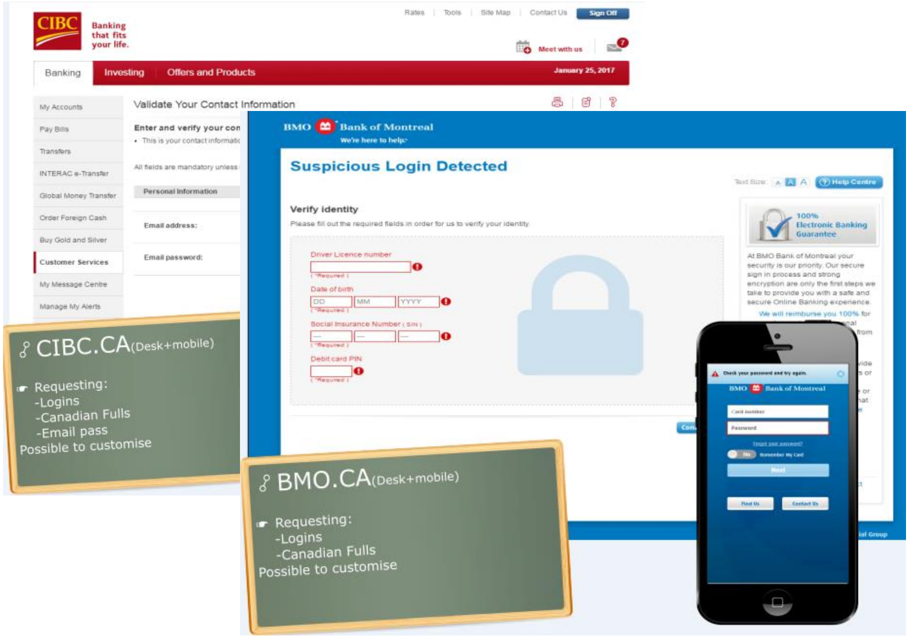
Vendor3: html is changed

Vendor3: the texts also

Vendor3: don't see a difference

The vendor sells ready-made phishing / injections packs for variety of countries and banks worldwide when the average price for 1 page is 50$. The ready injections/ phishing pages the vendor offers include the following:

- Canada - Pack of phishing pages for Canadian banks and credit cards collectors with admin panel on HTTPS domain and sets phishing pages - TD bank, CIBC, BMO, Desjardins Bank, RBC.



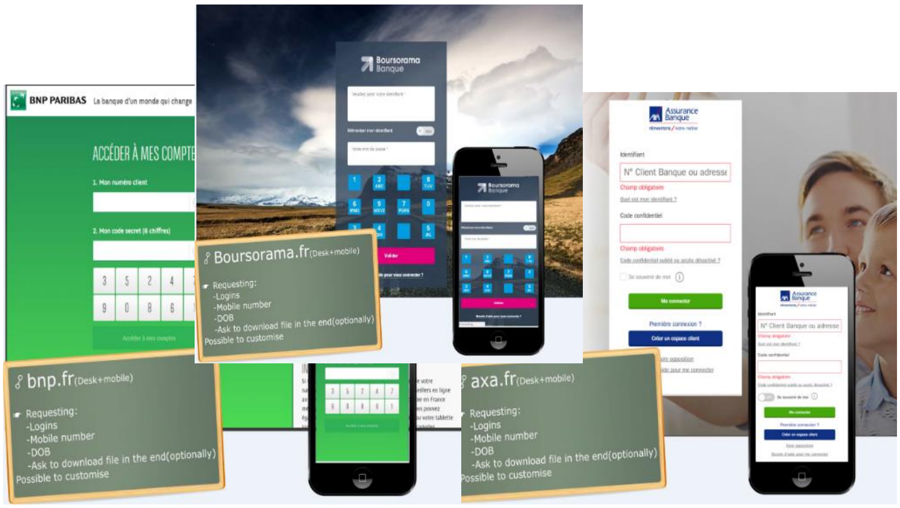
CIBC.CA(Desk+mobile)

Requesting:
-Logins
-Canadian Fulls
-Email pass
Possible to customise

BMO.CA(Desk+mobile)

Requesting:
-Logins
-Canadian Fulls
Possible to customise

- France - ready-made fake pages for different financial institutions including Assurance Banque, BNP Paribas, Boursorama Banque.



bnp.fr(Desk+mobile)

Requesting:
-Logins
-Mobile number
-DOB
-Ask to download file in the end(optionally)
Possible to customise

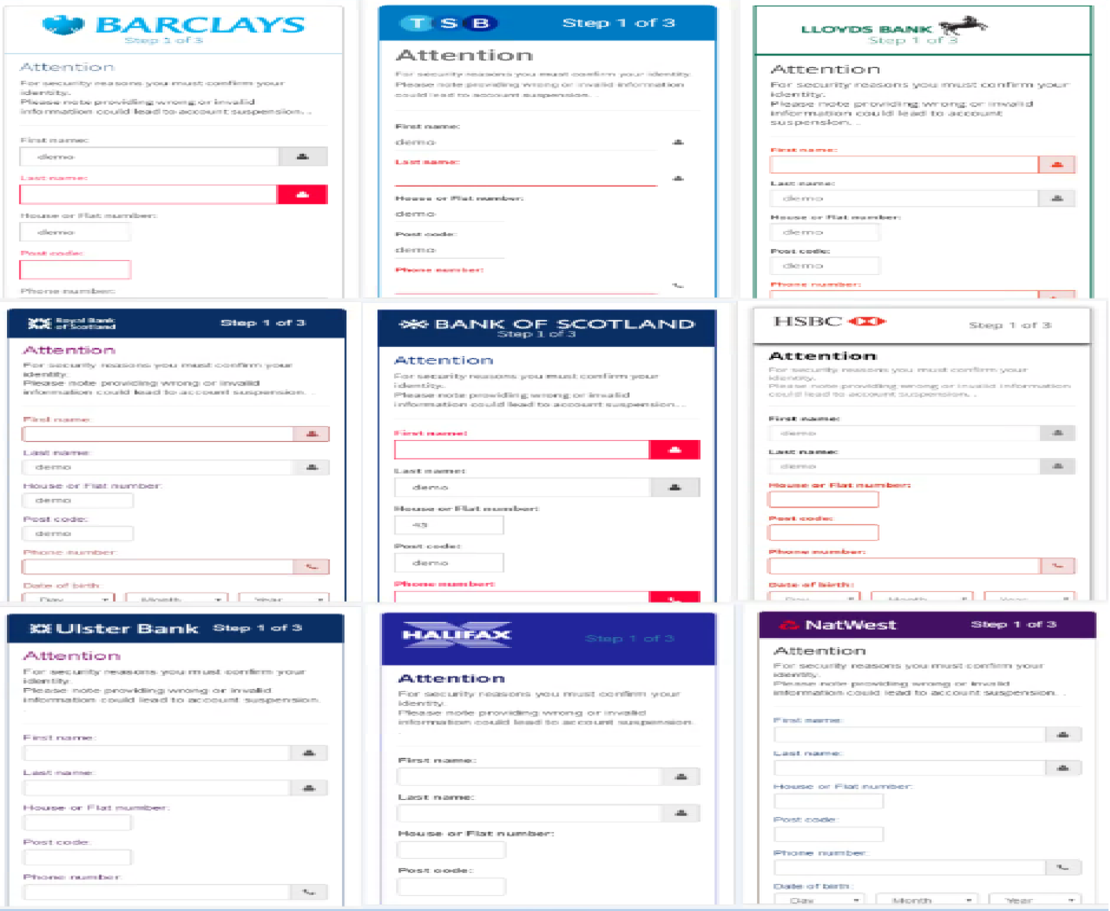
Boursorama.fr(Desk+mobile)

Requesting:
-Logins
-Mobile number
-DOB
-Ask to download file in the end(optionally)
Possible to customise

axa.fr(Desk+mobile)

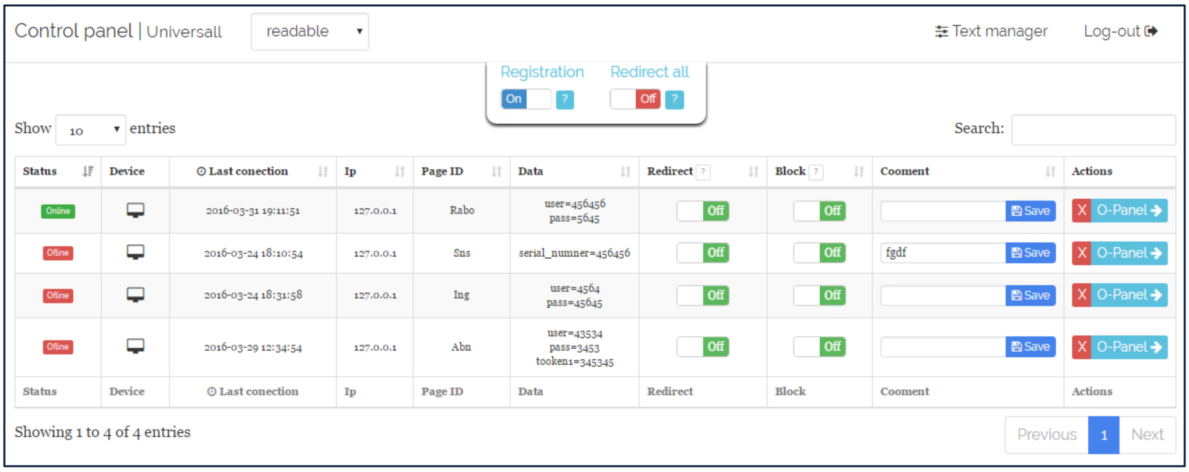
Requesting:
-Logins
-Mobile number
-DOB
-Ask to download file in the end(optionally)
Possible to customise

- UK - bank injects for android among them Barclays, TSB, Lloyds, Bank of Scotland, HSBC, Ulster bank, Halifax, NatWest and Royal bank of Scotland.



- Columbia - banks and Credit cards collectors with admin panel on https domain banks observed: Bancofalabella, Rbmcolombia, Colpatria, Bancolombia, Bancodeoccidente, Bancodebogota, Bbvanet, Bancopichincha
- Turkey
- Germany
- Thailand
- USA.

In addition, he sells “Universal Admin Panel” that can be integrated with different kinds of injections and phishing pages:



Control panel | Universall   readable ▾   Text manager   Log-out

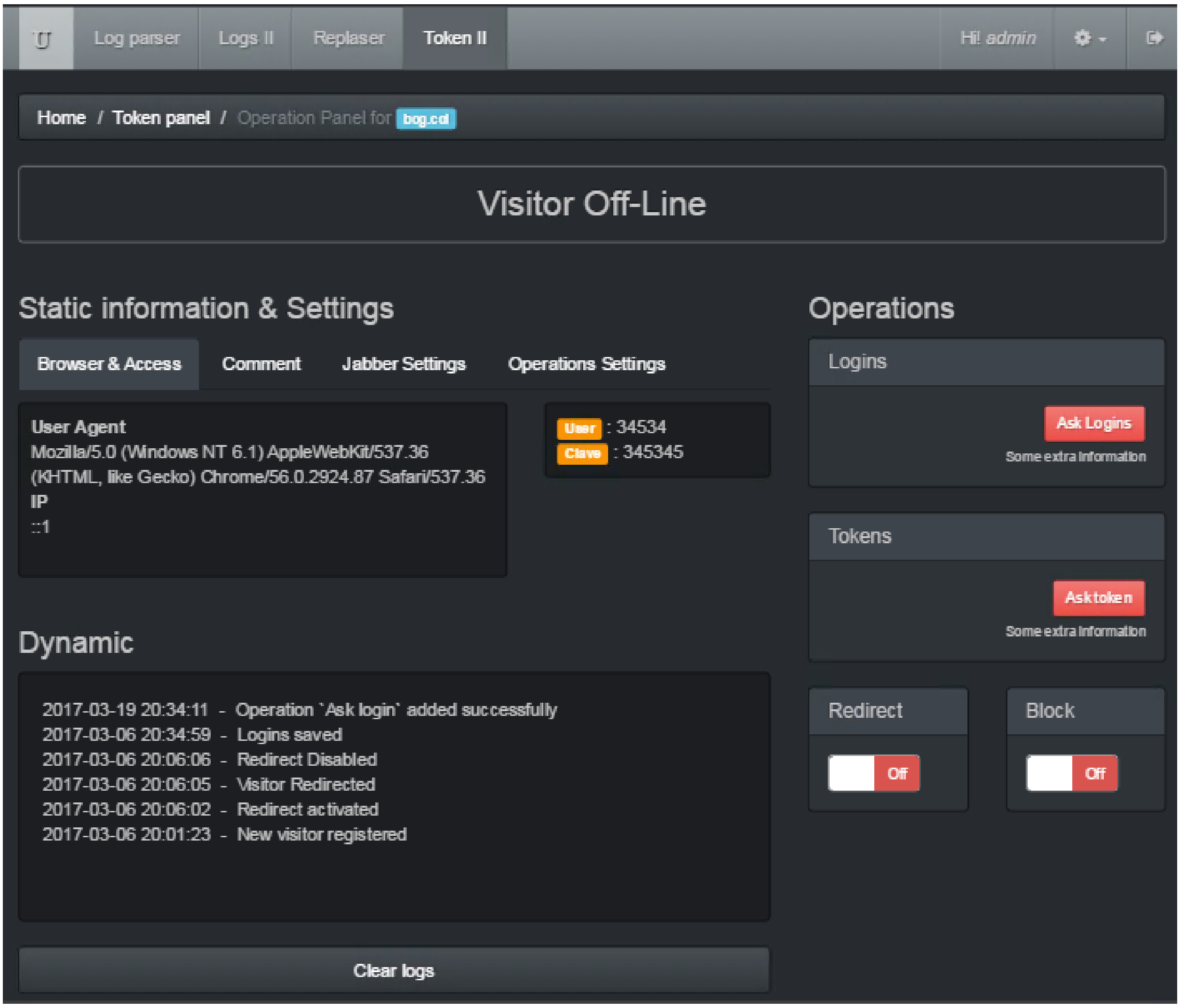
Registration: On ?   Redirect all: Off ?

Show 10 ▾ entries   Search:

Status	Device	Last conection	Ip	Page ID	Data	Redirect ?	Block ?	Coment	Actions
Online	🖥	2016-03-31 19:11:51	127.0.0.1	Rabo	user=456456 pass=5645	Off	Off	Save	X O-Panel
Ofline	🖥	2016-03-24 18:10:54	127.0.0.1	Sns	serial_numner=456456	Off	Off	fgdf Save	X O-Panel
Ofline	🖥	2016-03-24 18:31:58	127.0.0.1	Ing	user=4564 pass=45645	Off	Off	Save	X O-Panel
Ofline	🖥	2016-03-29 12:34:54	127.0.0.1	Abn	user=43534 pass=3453 tooken1=345345	Off	Off	Save	X O-Panel
Status	Device	Last conection	Ip	Page ID	Data	Redirect	Block	Coment	Actions

Showing 1 to 4 of 4 entries   Previous 1 Next

This panel allows to deal with real-time operations between the phishing operator and the visitor:



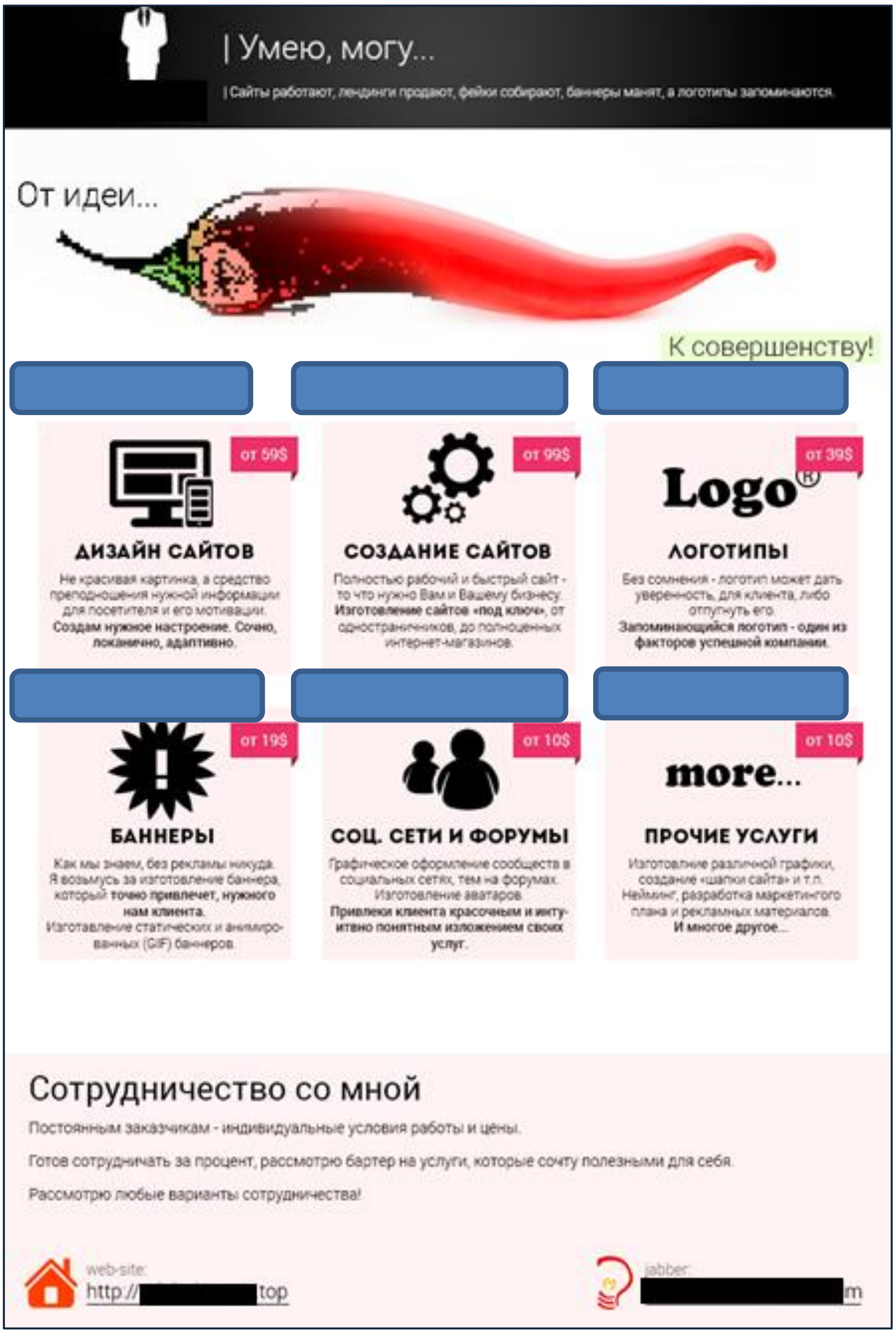
User Agent
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
IP
::1

User : 34534
Clave : 345345

```
2017-03-19 20:34:11  -  Operation `Ask login` added successfully
2017-03-06 20:34:59  -  Logins saved
2017-03-06 20:06:06  -  Redirect Disabled
2017-03-06 20:06:05  -  Visitor Redirected
2017-03-06 20:06:02  -  Redirect activated
2017-03-06 20:01:23  -  New visitor registered
```

Vendor4

Another vendor, “Vendor4”, launched in November 2016 new service on several forums under the following title : “Design from banner to portals !Websites, fakes, landing. Front-end web development, websites, creation of websites, banners , etc.” He also published the following



[redacted]

| Умею, могу...

| Сайты работают, лендинги продают, фейки собирают, баннеры манят, а логотипы запоминаются.

От идеи...

К совершенству!

[redacted] [redacted] [redacted]

от 59$

ДИЗАЙН САЙТОВ

Не красивая картинка, а средство преподношения нужной информации для посетителя и его мотивации. **Создам нужное настроение. Сочно, лоакнично, адаптивно.**

от 99$

СОЗДАНИЕ САЙТОВ

Полностью рабочий и быстрый сайт - то что нужно Вам и Вашему бизнесу. **Изготовление сайтов «под ключ»**, от одностраничников, до полноценных интернет-магазинов.

от 39$

Logo®

ЛОГОТИПЫ

Без сомнения - логотип может дать уверенность, для клиента, либо отпугнуть его. **Запоминающийся логотип - один из факторов успешной компании.**

[redacted] [redacted] [redacted]

от 19$

БАННЕРЫ

Как мы знаем, без рекламы никуда. Я возьмусь за изготовление баннера, который **точно привлечет, нужного нам клиента.** Изготавление статических и анимированных (GIF) баннеров.

от 10$

СОЦ. СЕТИ И ФОРУМЫ

Графическое оформление сообществ в социальных сетях, тем на форумах. Изготовление аватаров. **Привлеки клиента красочным и интуитивно понятным изложением своих услуг.**

от 10$

more...

ПРОЧИЕ УСЛУГИ

Изготовлние различной графики, создание «шапки сайта» и т.п. Нейминг, разработка маркетингого плана и рекламных материалов. **И многое другое...**

Сотрудничество со мной

Постоянным заказчикам - индивидуальные условия работы и цены.

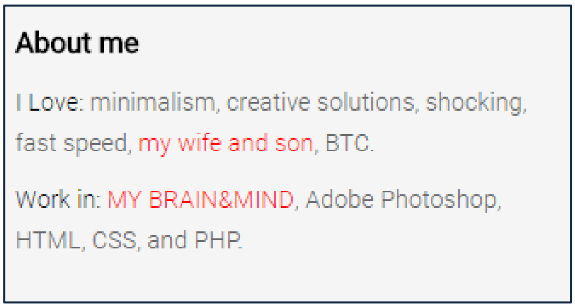
Готов сотрудничать за процент, рассмотрю бартер на услуги, которые сочту полезными для себя.

Рассмотрю любые варианты сотрудничества!

web-site:
http://[redacted]top

jabber:
[redacted]m

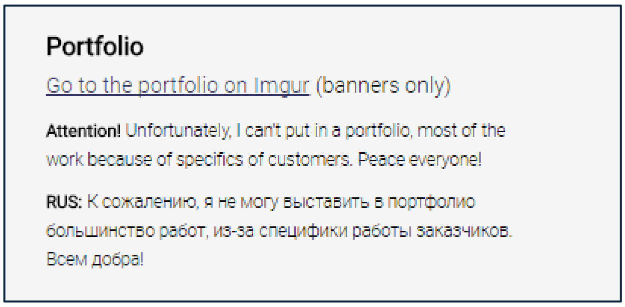
As part to promoting his services, and in addition to topics in several forums, he also created a website and there posted info about himself, and about his works :



About me

I Love: minimalism, creative solutions, shocking, fast speed, my wife and son, BTC.

Work in: MY BRAIN&MIND, Adobe Photoshop, HTML, CSS, and PHP.



Portfolio

Go to the portfolio on Imgur (banners only)

Attention! Unfortunately, I can't put in a portfolio, most of the work because of specifics of customers. Peace everyone!

RUS: К сожалению, я не могу выставить в портфолио большинство работ, из-за специфики работы заказчиков. Всем добра!

From a direct conversation with this vendor we see that he prefers not to do fakes for financial website, but specializes on making fakes to big corporate websites. He also emphasizes that he is not proficient in making validation of the stolen credentials against the original website/ servers.

ClearSky: I am contacting you regarding the fakes
Vendor4: somehow there is a hype today: D *Vendor4: for now bro I don't have time to another work, sorry, I'm overloaded with work*
ClearSky: it's not urgent
Vendor4: so, tell me)
ClearSky: want to ask for fakes pricing
Vendor4: fakes price begins from 100
*ClearSky: even such a simple fake as for online.***.co.** for example?*
Vendor4: and even this depends on the fake, there are some that I prefer not to do at all
ClearSky: do you develop or duplicate?
Vendor4: develop and write from scratch *Vendor4: such fakes – I prefer not to do at all – honestly, it is better to take those who specialize on them*
ClearSky: and fakes from scratch? *ClearSky: so, what is your specialty?*
Vendor4: I did such fakes for landing for CC grabbing, something else. Landings for (malicious – Clearsky) downloads, mostly fakes for corp. websites (duplicates or based on the original) for scamming.
ClearSky: shortly, everything except for banks
Vendor4: except for banks/retail/ social networks)
ClearSky: understand. Corp can be also relevant
Vendor4:)))
ClearSky: do you have some examples of your works?
Vendor4: I will say in such way. Have but haven't, at the same time ;) have feedback in (redacted - Clearsky) *Vendor4: it will be easier in such a way. Say what is required and I will say whether it is possible or not. the price and the terms.*
ClearSky: 2 things (not urgent). *ClearSky: 1. Login page for corporate mail* *ClearSky: 2. Full corporate website, that has 2-3 different login page*

Vendor4: do you need validation or the forms content or simply to put the entered credentials to file/mail?

Vendor4: why I don't like fakes. If it is required just to make logs of the data from the forms (to txt or to mail) – welcome, I can do it. If it is required to do validation of the credentials on the original server, it is not for me. Better talk with those who specialize on this) will be done faster and will cost less) I simply don't have time to deal with this. Understand me.

Vendor4: things that I'm proficient in, I do good and properly, what I'm not – and don't have time to study (because of high amount of work), so better I'll refuse than not keeping the deadline and losing my reputation

ClearSky: in one page, there is a small verification for validity

ClearSky: and the full corp. website – no need for validation

ClearSky: what is the approximate price for such a website?

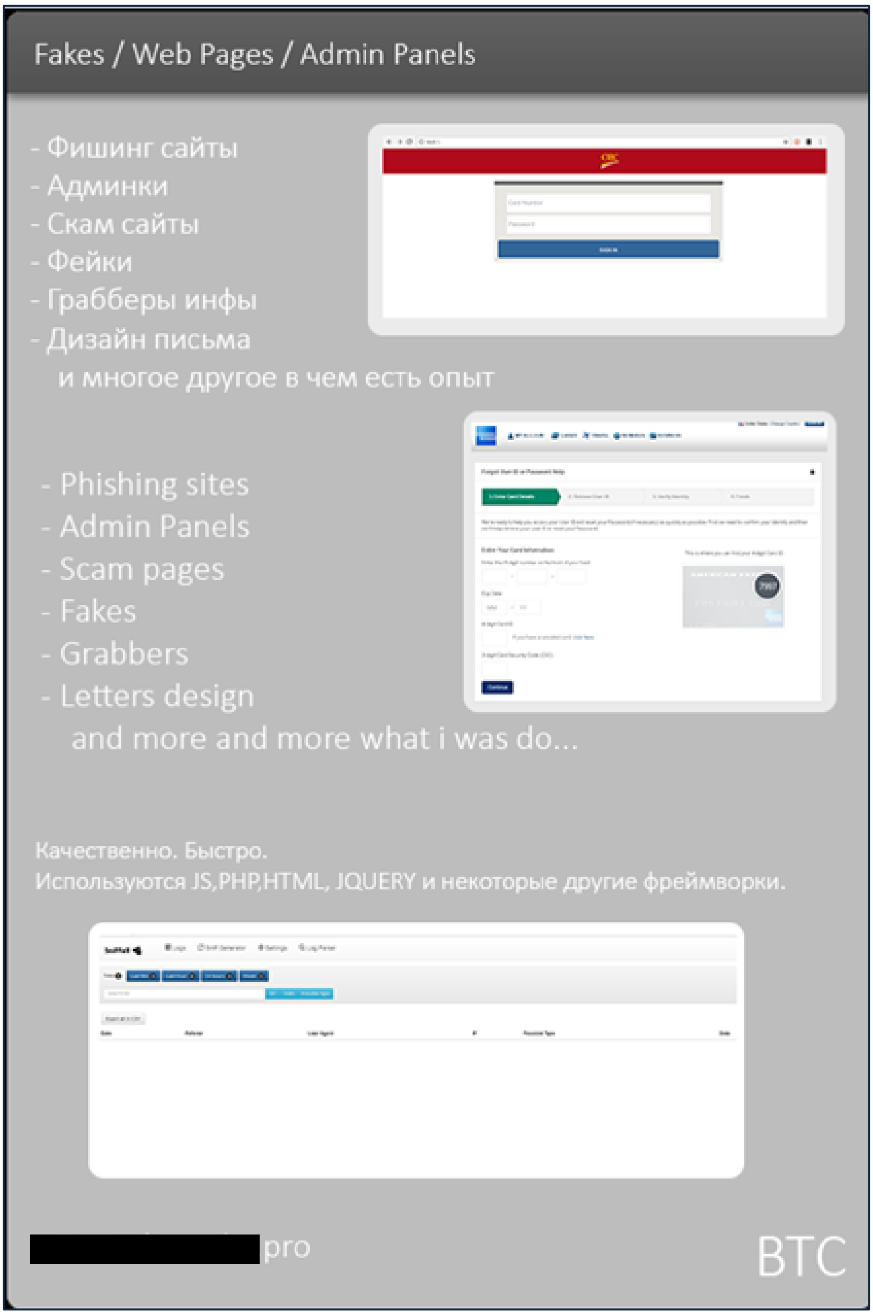
Vendor4: if the validation is on the side of the original server (i.e. can such a user enter to the original website – so ok. If otherwise – so stop) – I can't do it currently)

Vendor4: (the price – Clearsky) depends on the website, how many pages, complexity of its development (as I said, I make it from the scratch, fit it for the original – so if there will be changes, nothing will look out of the ordinary

Vendor4: it begins from 100, till fuck knows how much it can be) depends on the original, on work volume.

Vendor5

Another subject is verified seller *"Vendor5"* that began offering his services in 2015 and advertises himself via the following:



Fakes / Web Pages / Admin Panels

- Фишинг сайты
- Админки
- Скам сайты
- Фейки
- Грабберы инфы
- Дизайн письма

и многое другое в чем есть опыт

- Phishing sites
- Admin Panels
- Scam pages
- Fakes
- Grabbers
- Letters design

and more and more what i was do...

Качественно. Быстро.
Используются JS,PHP,HTML, JQUERY и некоторые другие фреймворки.

[redacted]pro

BTC

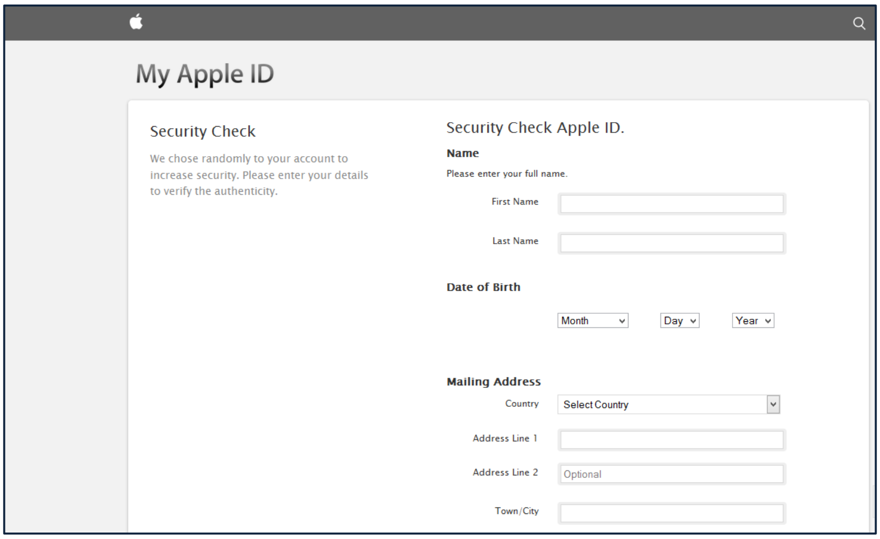
The vendor posted that he copies the needed sites, with required changes, beginning from 50$. He emphasized that his fakes survive for a long time because mostly he develops the required page from scratch, and not duplicates it as most "developers".

He also presents possible functionalities and add-ons to his services :

> *>>>Delimitation of user permissions (access to specific parts or functionalities)*
> *>>> Hosting on .onion*
> *>>> Deposit of balance through BTC*
> *>>> Ticketing system with live updates*
> *>>> Defense from SQLi and XSS attacks*

As part of advertising his services and showing his abilities, he also presents several ready-made high-quality fakes for the most popular websites and services:

1. Apple



My Apple ID

Security Check

We chose randomly to your account to increase security. Please enter your details to verify the authenticity.

Security Check Apple ID.

Name

Please enter your full name.

First Name

Last Name

Date of Birth

Month Day Year

Mailing Address

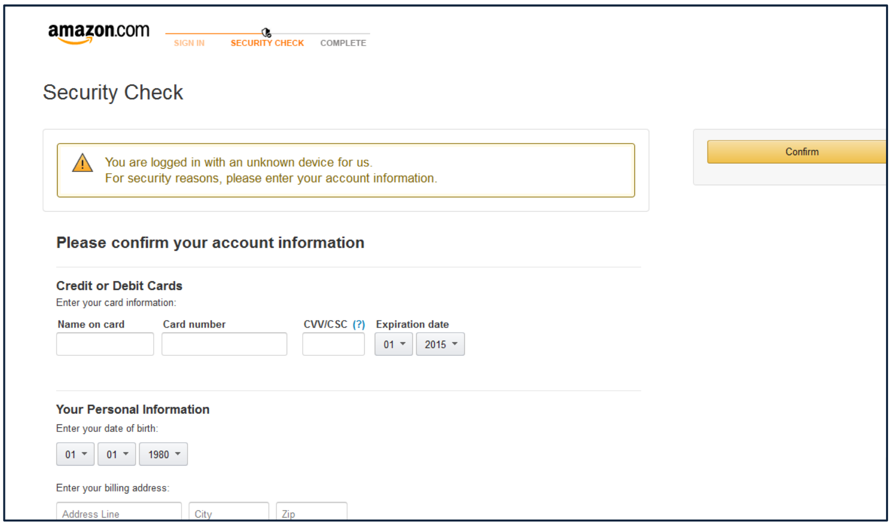
Country: Select Country

Address Line 1

Address Line 2: Optional

Town/City

2. Amazon



Security Check

You are logged in with an unknown device for us.
For security reasons, please enter your account information.

Please confirm your account information

Credit or Debit Cards

Enter your card information:

Name on card | Card number | CVV/CSC (?) | Expiration date: 01 2015

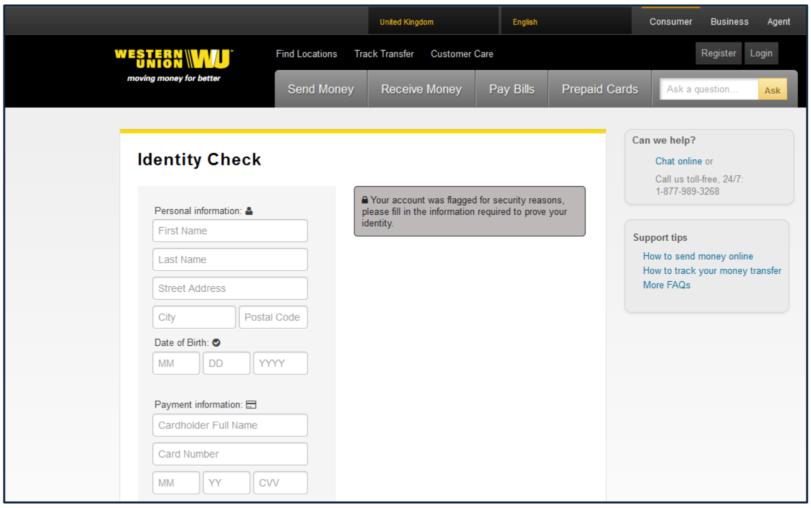
Your Personal Information

Enter your date of birth: 01 01 1980

Enter your billing address:

Address Line | City | Zip

3. Western Union



Identity Check

Personal information:

First Name

Last Name

Street Address

City | Postal Code

Date of Birth:

MM | DD | YYYY

Payment information:

Cardholder Full Name

Card Number

MM | YY | CVV

Your account was flagged for security reasons, please fill in the information required to prove your identity.

Can we help?

Chat online or

Call us toll-free, 24/7:
1-877-989-3268

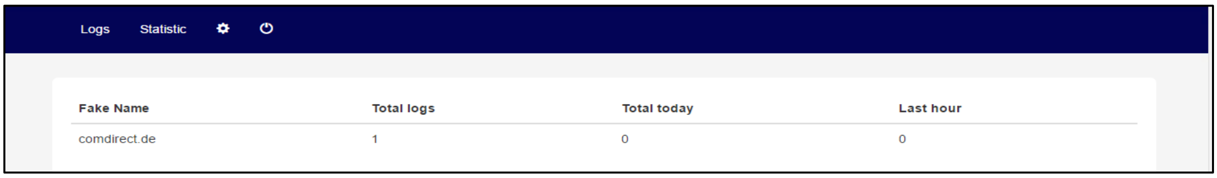
Support tips

How to send money online
How to track your money transfer
More FAQs

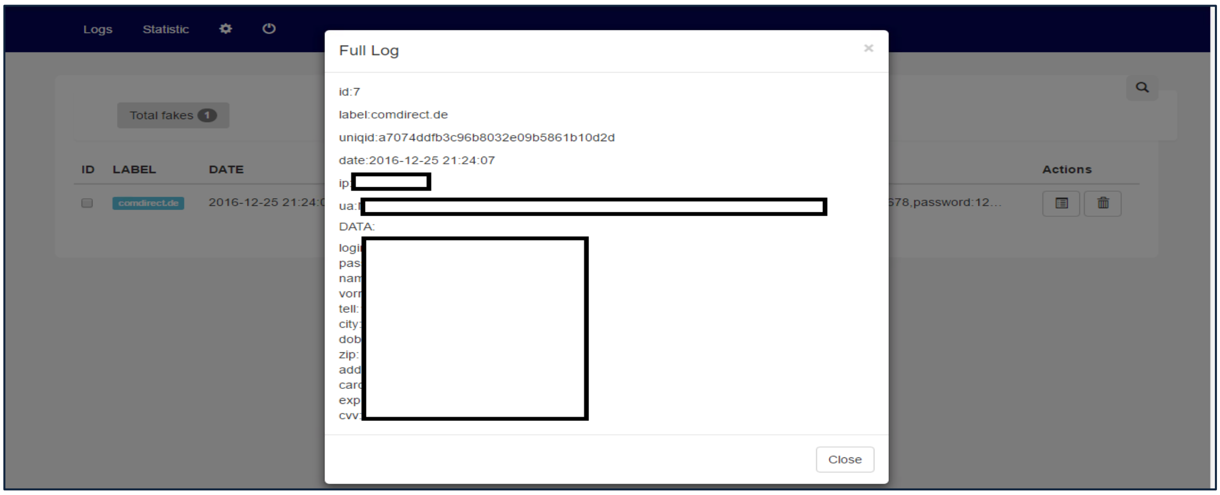
In addition, he specifies, that he has ready fakes also for the following sites and services:

1. Paypal, including automated language selection
2. Visa
3. Suntrust Bank
4. UK banks
5. Gmail
6. Landing page for Flash Player

This vendor also presented admin panels that he attaches to the fake websites and help to collect the stolen credentials:



Fake Name	Total logs	Total today	Last hour
comdirect.de	1	0	0



ID	LABEL	DATE
	comdirect.de	2016-12-25 21:24:(

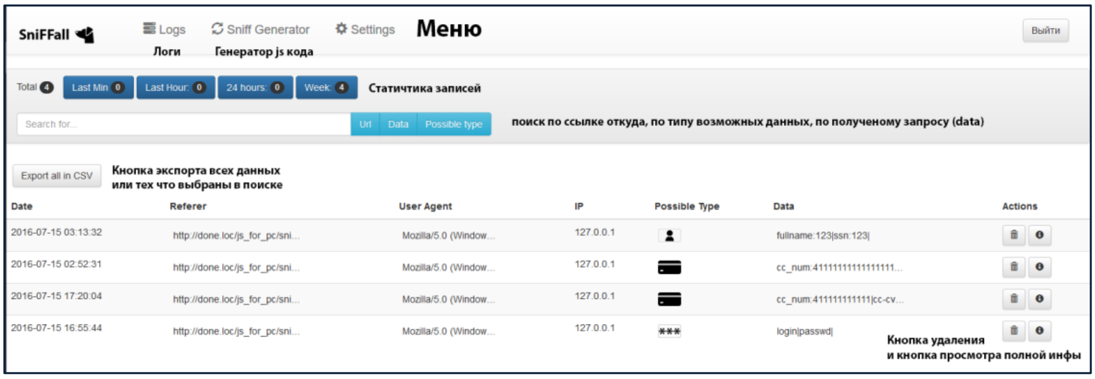
578,password:12...

Full Log

id:7
label:comdirect.de
uniqid:a7074ddfb3c96b8032e09b5861b10d2d
date:2016-12-25 21:24:07
ip [redacted]
ua: [redacted]
DATA:
logi
pas
nam
vorr
tell:
city:
dob
zip:
add
card
exp
cvv:
[redacted]

As we see this vendor is a specialist for different kinds of services and products and during June 2016, he also launched new product – “SniFFall”, universal sniffer of CC, passwords of controlled websites.

It works by inserting small JS code to the website and receiving to the admin panel all the requests and forms filled in the page that includes the JS code. The cost of this component was 250$.



Меню

Логи

Генератор js кода

Статичтика записей

поиск по ссылке откуда, по типу возможных данных, по полученому запросу (data)

Кнопка экспорта всех данных
или тех что выбраны в поиске

Date	Referer	User Agent	IP	Possible Type	Data	Actions
2016-07-15 03:13:32	http://done.loc/js_for_pc/sni...	Mozilla/5.0 (Window...	127.0.0.1	👤	fullname:123|ssn:123|	🗑 ℹ
2016-07-15 02:52:31	http://done.loc/js_for_pc/sni...	Mozilla/5.0 (Window...	127.0.0.1	💳	cc_num:41111111111111111...	🗑 ℹ
2016-07-15 17:20:04	http://done.loc/js_for_pc/sni...	Mozilla/5.0 (Window...	127.0.0.1	💳	cc_num:411111111111|cc-cv...	🗑 ℹ
2016-07-15 16:55:44	http://done.loc/js_for_pc/sni...	Mozilla/5.0 (Window...	127.0.0.1	***	login|passwd|	🗑 ℹ

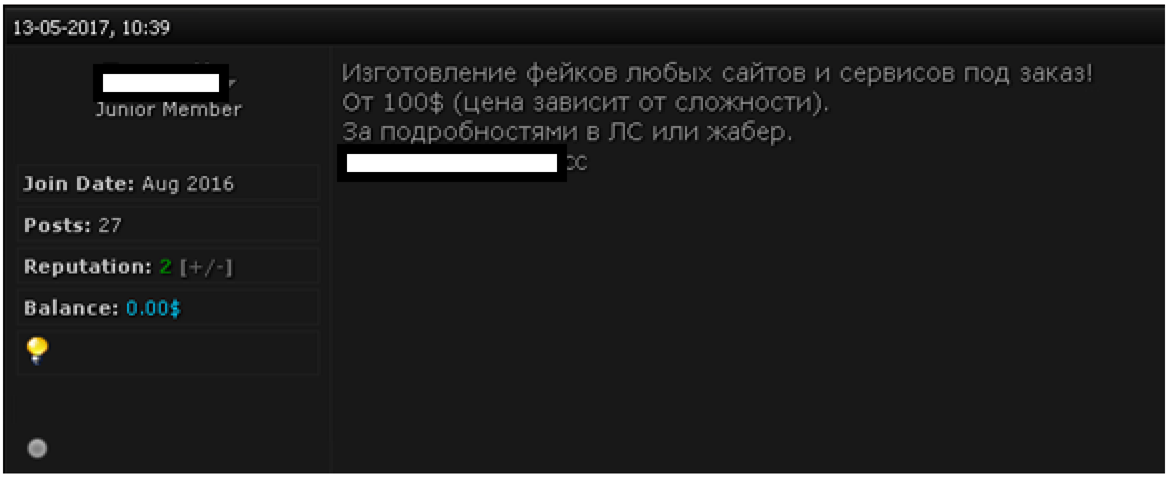
Кнопка удаления
и кнопка просмотра полной инфы

From conversation with the vendor, we can see that his prices for a simple banking fake are relatively high (about 200$), this due to the fact that he develops the website from scratch and adds some filters against botnets and scanners that prolong to the life of the website:

ClearSky: I'm regarding the fakes
Vendor5: hearing you
ClearSky: want to ask the pricing for relatively simple *ClearSky: for example for ***bank*
Vendor5: describe
*ClearSky: fake for online.***bank.***
Vendor5: what to collect?
ClearSky: user id and pass
Vendor5: it will cost at least 200 *Vendor5: I don't duplicate the site* *Vendor5: but develop it from scratch* *Vendor5: myself*
ClearSky: how much does it reduce the chance of the site to be exposed? *ClearSky: because there are some who offer it for 30-50*
Vendor5: good for them *Vendor5: will significantly reduce* *Vendor5: I have also another filter* *Vendor5: the life time is significantly longer*
ClearSky: which filter?
Vendor5: as a defense from different bots *Vendor5: and scanners*
ClearSky: for every bank such a fake costs 200? *ClearSky: or possible also cheaper?*
Vendor5: cheaper is almost impossible *Vendor5: to give away my techniques for lower price doesn't make any sense.*
ClearSky: clear. *ClearSky: what are the deadlines for such a work?*
Vendor5: maximum 2-3 days *Vendor5: sometimes I can do it within 2 hours* *Vendor5: depends on my workload*
ClearSky: and if I'll add to the fake another page (second stage) for cc+cvv…for how much it rises the price?
Vendor5: it will cost 250

Vendor6

Vendor by the name “Vendor6” offers fakes development, for price beginning from 100$, depends on the complexity:



13-05-2017, 10:39

[redacted]
Junior Member

Join Date: Aug 2016

Posts: 27

Reputation: 2 [+/-]

Balance: 0.00$

Изготовление фейков любых сайтов и сервисов под заказ!
От 100$ (цена зависит от сложности).
За подробностями в ЛС или жабер.
[redacted]

From conversation with the vendor, we see that he is a fresh service provider who don’t even have examples of his works to provide, but his pricing is relatively high and is about 150$ for banking fake and credit cards grabbing:

ClearSky: I’m regarding the fakes

Vendor6: full description of what is required, deadlines, financial capacities.

…

*ClearSky: fake of banking login like online. ***bank.co.** + additional page for CC*
ClearSky: not urgent

Vendor6: 3-4 days 150$

ClearSky: and if only the login page?

Vendor6: without hurry and doing it right - will work for weeks
Vendor6: 100

ClearSky: do you develop it or duplicate?

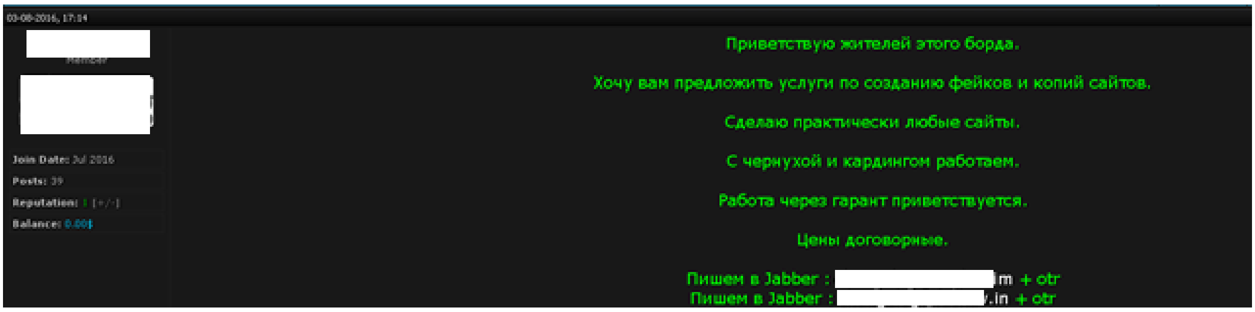
Vendor6: depends on the complexity

ClearSky: do you have some examples of works or feedback?

Vendor6: if it is impossible to extract all the scripts, so I develop it
Vendor6: I just started providing the service
Vendor6: in several days, I finish a project
Vendor6: so you will have a demo

Vendor7

Another vendor, “Vendor7”, beginning from August 2016, offers services of fake websites creation and advertises his services in more than 10 different Russian underground forums



03-08-2016, 17:14

[redacted]

[redacted]

Join Date: Jul 2016

Posts: 39

Reputation: 1 [+/-]

Balance: 0.00$

Приветствую жителей этого борда.

Хочу вам предложить услуги по созданию фейков и копий сайтов.

Сделаю практически любые сайты.

С чернухой и кардингом работаем.

Работа через гарант приветствуется.

Цены договорные.

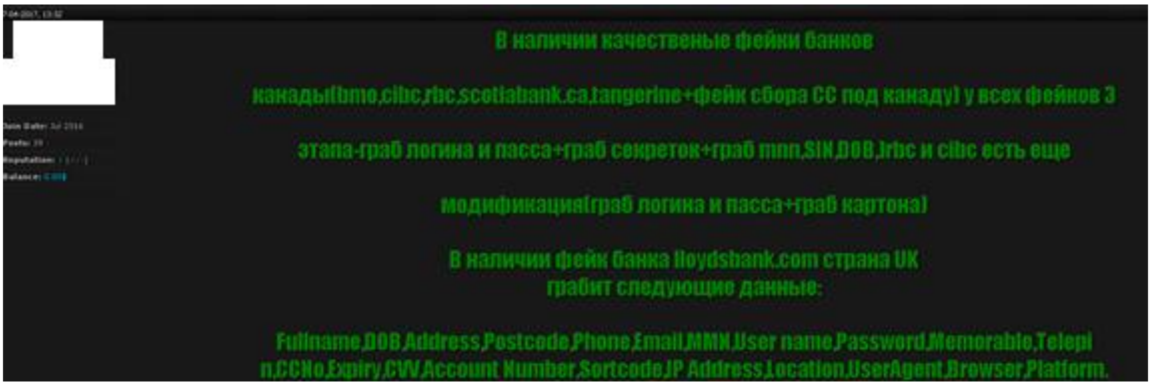
Пишем в Jabber : [redacted]m + otr
Пишем в Jabber : [redacted].in + otr

In addition, he offers ready high-quality fakes of Canada banks (BMO, CIBC, RBC, Scotiabank, Tangerine) and fakes for Credit Cards collection in Canada. He explains, that all those the fakes have 3 stages:

1. Grabbing of login and password
2. Grabbing of credit card numbers and CVV
3. Grabbing of MNN, Social Insurance number(SIN) and Date of Birth (DOB)

In addition, he mentions that he has ready fake for Lloydsbank, UK that grabs the following information:

Fullname	Email	CCNo	IPAddress
DOB	MMN	Expiry	Location
Address	Username	CVV	UserAgent
Postcode	Password	Sortcode	AccountNumber
Phone	Telepin		BrowserandPlatform



[redacted]

Join Date: Jul 2016

Posts: 39

Reputation: 1 [+/-]

Balance: 0.00$

В наличии качественые фейки банков

канады(bmo,cibc,rbc,scotiabank.ca,tangerine+фейк сбора CC под канаду) у всех фейков 3

этапа-граб логина и пасса+граб секретов+граб mnn,SIN,DOB,(rbc и cibc есть еще

модификация(граб логина и пасса+граб картона)

В наличии фейк банка lloydsbank.com страна UK
грабит следующие данные:

Fullname,DOB,Address,Postcode,Phone,Email,MMN,User name,Password,Memorable,Telepi
n,CCNo,Expiry,CVV,Account Number,Sortcode,IP Address,Location,UserAgent,Browser,Platform.

In one of one conversation, the vendor presents several of his works (credit cards and banking accounts shops) and states that the price for basic fake is about 30$, but if there is requirement for a more complicated fake – it will cost 250$.

ClearSky: I’m regarding the fakes
Vendor7: hi. I’m listening
ClearSky: I would like to know the pricing for relatively simple fake
Vendor7: relatively simple is a relative term. better write the terms of reference
*ClearSky: e.g. online.***bank.***
Vendor7: simply grabbing of the login and the password?
ClearSky: yes

Vendor7: 30$

ClearSky: are you duplicating or developing?

Vendor7: duplicating, with development it will be more expensive

ClearSky: those that are duplicated are being exposed very quickly

ClearSky: and how much with development?

Vendor7: now I'm doing as a trial a fake with development. Tomorrow will update when it is finished – whether succeed in it or not. another bank I'm doing tomorrow and will update on the exact price

Vendor7: Now I'm exactly doing a bank (fake – ClearSky) which is being exposed after 1-2 minutes of being in browser

….

ClearSky: and if I add to the fake another page (second stage) for (collecting -Clearsky) cc + cvv … how it rises the price?

Vendor7: such complete fake, with cards gathering + anything else you need will cost 250$

Vendor7: it is developed

ClearSky: understood. Do you have some examples of your works, or feedback?

Vendor7: examples of my works :

https://***.cc/ - CC shop

http://***-market.cc/ - Bank accounts shop

https://****exchangebit.me/ - Egift shop

Vendor7: logs are to be sent to mail?

ClearSky: prefer so, but if there is a big difference in the price – possible txt

Vendor7: no difference, as you prefer

…

ClearSky: do also do fakes for corp. websites?

Vendor7: yes

Vendor7: show an example of what needed

ClearSky: http://www.****.org/ + https://member.****.org

The conversation took more than one day, and consisted of checking the possibility to conduct a fake for complex corporate site, to impersonate big corporation – the vendor asked for this work 150$:

ClearSky: the second thing is corporate website

Vendor7:

https://member.****.org/_layouts/****/SPI/shell/login.aspx?ReturnUrl=

%2f_layouts%2fAuthenticate.aspx% 3fSource%3d%252F&Source=%2F

here is required to grab only mail and pass?

Vendor7: it also should be developed?

ClearSky: yes, and yes. But also, the main website is required

ClearSky: how much it will cost?

Vendor7: so there will be the main page and another one with the grab. Other links to forward to the original or to develop all the pages?

ClearSky: need all the pages

Vendor7: let's now go over the details and afterwards I will say the price

Vendor7: so wait a min, I will check

ClearSky: ок

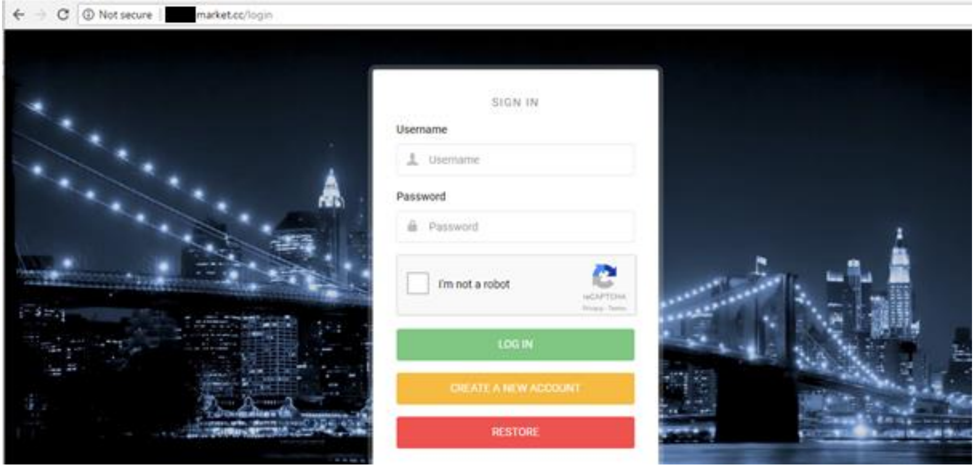
Vendor7: see, I checked now the corp. website and think it makes no sense to do it with screenshots, they don't have any normal defense on the website. And it will cost less to you. Regarding the bank – of course with screenshots. The corp. website will cost 150$ (there are many pages to be ripped) and the fake 250$, will be developed

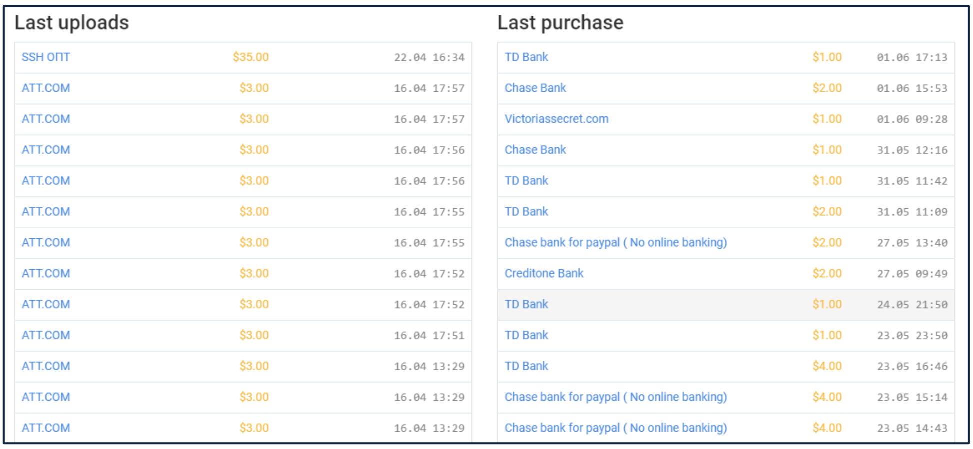
Vendor7: will try to do it within 3 days

*Vendor7: http://prntscr.com/**** I already ripped one page, to check what it going on there*

Apart of conducting regular fakes he also makes online shops with different payments possibilities, of course for illegal purposes like money laundering, cashing out virtual credit cards, etc.

He presents an example of one of his works, accounts market:





Last uploads			Last purchase		
SSH ОПТ	$35.00	22.04 16:34	TD Bank	$1.00	01.06 17:13
ATT.COM	$3.00	16.04 17:57	Chase Bank	$2.00	01.06 15:53
ATT.COM	$3.00	16.04 17:57	Victoriassecret.com	$1.00	01.06 09:28
ATT.COM	$3.00	16.04 17:56	Chase Bank	$1.00	31.05 12:16
ATT.COM	$3.00	16.04 17:56	TD Bank	$1.00	31.05 11:42
ATT.COM	$3.00	16.04 17:55	TD Bank	$2.00	31.05 11:09
ATT.COM	$3.00	16.04 17:55	Chase bank for paypal (No online banking)	$2.00	27.05 13:40
ATT.COM	$3.00	16.04 17:52	Creditone Bank	$2.00	27.05 09:49
ATT.COM	$3.00	16.04 17:52	TD Bank	$1.00	24.05 21:50
ATT.COM	$3.00	16.04 17:51	TD Bank	$1.00	23.05 23:50
ATT.COM	$3.00	16.04 13:29	TD Bank	$4.00	23.05 16:46
ATT.COM	$3.00	16.04 13:29	Chase bank for paypal (No online banking)	$4.00	23.05 15:14
ATT.COM	$3.00	16.04 13:29	Chase bank for paypal (No online banking)	$4.00	23.05 14:43

Vendor8

Another vendor that we checked was Vendor8, that offers his services from May 2016. He states that he also has experience working with DB's. In his initial posts he didn't mentioned the pricing, so we contacted him via jabber:

ClearSky: I'm regarding the fakes

Vendor8: a set of fakes?

ClearSky: fake of bank login…

Vendor8: it requires development?

ClearSky: at first, fake of an existing page

Vendor8: I'm occupied now with development of my panel, will be available in 3-4 days
Vendor8: maybe even sooner

ClearSky: ok
ClearSky: are you duplicating or developing?

Vendor8: duplicating, but if there are any errors in the original – I'm trying to develope it from scratch
Vendor8: so mostly, my fakes has 100% similarity

ClearSky: it includes cleaning, so the site will have less chances to be exposed?

Vendor8: if cleaning is removal of unnecessary from the original, so can do it

ClearSky: what are the prices?

Vendor8: the price is negotiable

*ClearSky: for example, fake of online.***bank.** how much will cost?*

Vendor8: here is required to steal the user is and password?

ClearSky: exactly.

Vendor8: it depends on the problems that can arise during the development
Vendor8: the price depends on it

ClearSky: what is the minimum and the maximum?
ClearSky: approximately

Vendor8: minimum 1k maximum 2.5 k
Vendor8: around this
Vendor8: if it is urgent I can do it now

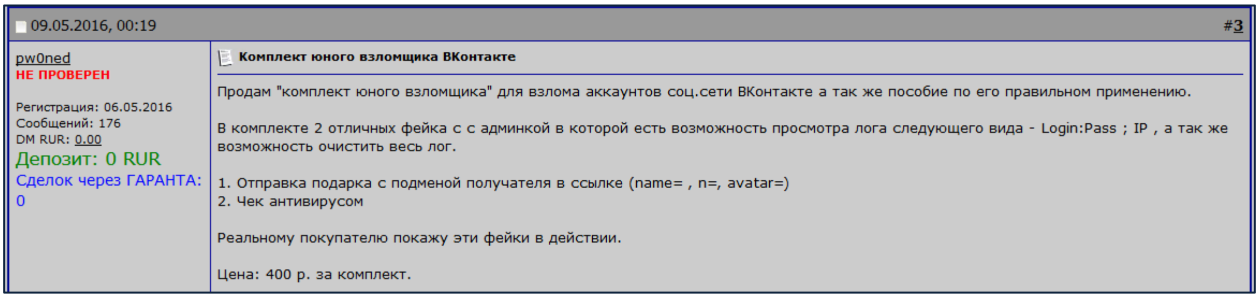
ClearSky: in what currency?

Vendor8: if there are no complications, the work will be done within 10-20 minutes
Vendor8: rubles

ClearSky: no…not urgent
ClearSky: do you have examples of works that you can present?

*Vendor8: I don't save the fakes of the clients, but I have enough feedbacks, also I passed the verification in ****/**** (2 forums names – Clearsky)*
*Vendor8: feedbacks in ***, ***, ***, **** (4 forums names – Clearsky)*

He also offers ready fakes set for VK, leading Russian social network that includes 2 fake pages and admin panel for a really cheap price of about 7$:



09.05.2016, 00:19 #3

pw0ned
НЕ ПРОВЕРЕН

Регистрация: 06.05.2016
Сообщений: 176
DM RUR: 0.00
Депозит: 0 RUR
Сделок через ГАРАНТА: 0

Комплект юного взломщика ВКонтакте

Продам "комплект юного взломщика" для взлома аккаунтов соц.сети ВКонтакте а так же пособие по его правильном применению.

В комплекте 2 отличных фейка с с админкой в которой есть возможность просмотра лога следующего вида - Login:Pass ; IP , а так же возможность очистить весь лог.

1. Отправка подарка с подменой получателя в ссылке (name= , n=, avatar=)
2. Чек антивирусом

Реальному покупателю покажу эти фейки в действии.

Цена: 400 р. за комплект.

Vendor9

In April 2017, another vendor offered services of developing complicated fakes and landings for almost every theme, all of this is developed based on PHP, with prices that start from 50$. During a conversation, we have seen that he is ready to lower his priced in exchange for positive feedback in the forums.

ClearSky: I'm regarding the fakes
ClearSky: I want to know the prices for relatively simple
*ClearSky: like online.***bank. ***

Vendor9: verification of the login/password
Vendor9: is required?

ClearSky: possible without…

Vendor9: with/without deployment?

ClearSky: with

Vendor9: VPS/Shared?
Vendor9: the domain connected?

ClearSky: shared

Vendor9: the logs are to mail
Vendor9: or locally into .txt?

ClearSky: yes… will be connected

Vendor9: user agent + time + log/pass
Vendor9: will do for 40$, if will include feedback)

ClearSky: are you duplicating or developing?

Vendor9: it is foolish to duplicate – will be exposed immediately
Vendor9: in chrome/safari
Vendor9: I'm developing myself

ClearSky: ok
ClearSky: and if I add another page for CC gathering?

Vendor9: show an example

ClearSky: to develop a page with the same bank's template, that will ask to enter cc+exp+cvv

Vendor9: after the input of login/password you mean?

ClearSky: yes

Vendor9: for mobile/desktop?
Vendor9: to make a cross platform development?

ClearSky: desktop

Vendor9: in short, to develop with the same style of the bank, right?

ClearSky: yes
ClearSky: what will be the price?

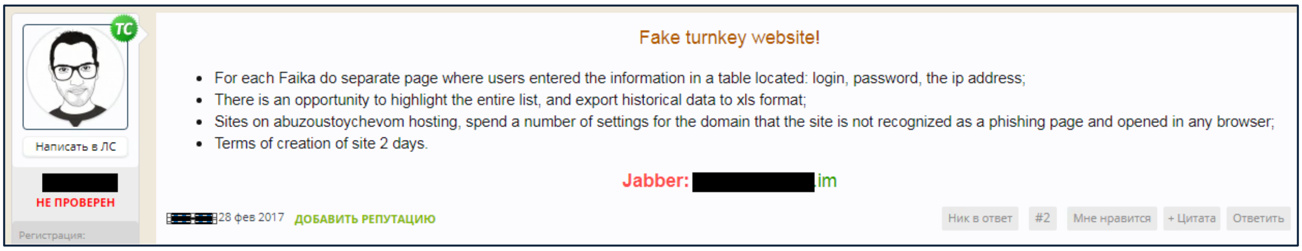
Vendor9: hmm…it will cost 100$
Vendor9: I'm ready to divide escrow fee 50/50

ClearSky: do you have work examples? Or feedback?

Vendor9: I do have freelance, but I will not show it
Vendor9: there is my personal old profile

Vendor10

Another vendor offers his services for creating fakes, and fake templates beginning February 2017.



Fake turnkey website!

- For each Faika do separate page where users entered the information in a table located: login, password, the ip address;
- There is an opportunity to highlight the entire list, and export historical data to xls format;
- Sites on abuzoustoychevom hosting, spend a number of settings for the domain that the site is not recognized as a phishing page and opened in any browser;
- Terms of creation of site 2 days.

Jabber: [redacted].im

[redacted]28 фев 2017

Although this post was published in English, it is obvious that his English level is very low. In addition to specific fakes that can be ordered from him, he also offers ready phishing scam pages for Bank of America, HSBC, PayPal, Gmail (set of all the four for 150$).

On direct conversation with the vendor, he told us that banking login page fake, and second stage for credit cards grabbing costs about 70$, when the fake is mostly developed and not duplicated.

ClearSky: yes…I want to ask what the prices for fake are

Vendor10: 70$, including the deployment
Vendor10: short Terms of Reference is required, what is needed to be done, what should be saved

ClearSky: what do you mean? Including hosting?

Vendor10: yes

ClearSky: the price for 1 or 2 pages is the same?

Vendor10: the same, the second page is mainly for authorization, approval
Vendor10: the deadlines are about 1-2 days

ClearSky: and if the first page grabs bank login and the second grabs CC?

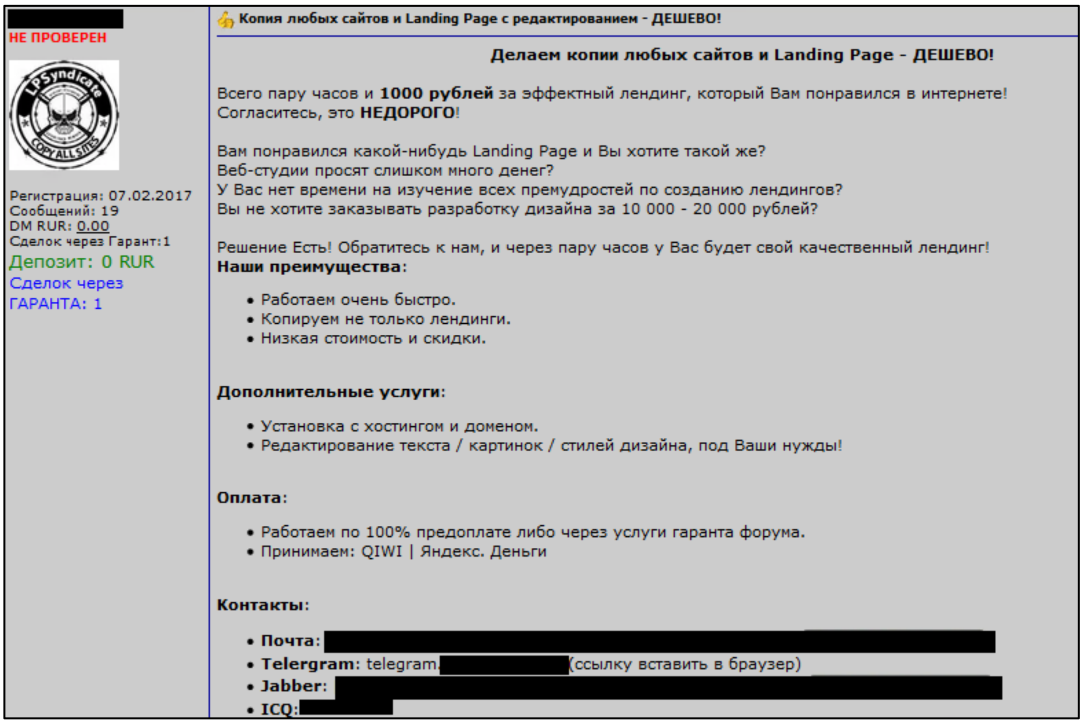
Vendor10: right
Vendor10: it is what I meant

ClearSky: are you duplicate or develop from scratch?

Vendor10: develop
Vendor10: some elements we copy

Vendor11

From February 2017 another vendor, offers in Russia speaking communities, services of fake and landing pages creation, for price of 1000 rubles only (about 17$), within several hours as he promises:



[redacted]
НЕ ПРОВЕРЕН

Регистрация: 07.02.2017
Сообщений: 19
DM RUR: 0.00
Сделок через Гарант:1
Депозит: 0 RUR
Сделок через ГАРАНТА: 1

Копия любых сайтов и Landing Page с редактированием - ДЕШЕВО!

Делаем копии любых сайтов и Landing Page - ДЕШЕВО!

Всего пару часов и **1000 рублей** за эффектный лендинг, который Вам понравился в интернете!
Согласитесь, это **НЕДОРОГО**!

Вам понравился какой-нибудь Landing Page и Вы хотите такой же?
Веб-студии просят слишком много денег?
У Вас нет времени на изучение всех премудростей по созданию лендингов?
Вы не хотите заказывать разработку дизайна за 10 000 - 20 000 рублей?

Решение Есть! Обратитесь к нам, и через пару часов у Вас будет свой качественный лендинг!
Наши преимущества:

- Работаем очень быстро.
- Копируем не только лендинги.
- Низкая стоимость и скидки.

Дополнительные услуги:

- Установка с хостингом и доменом.
- Редактирование текста / картинок / стилей дизайна, под Ваши нужды!

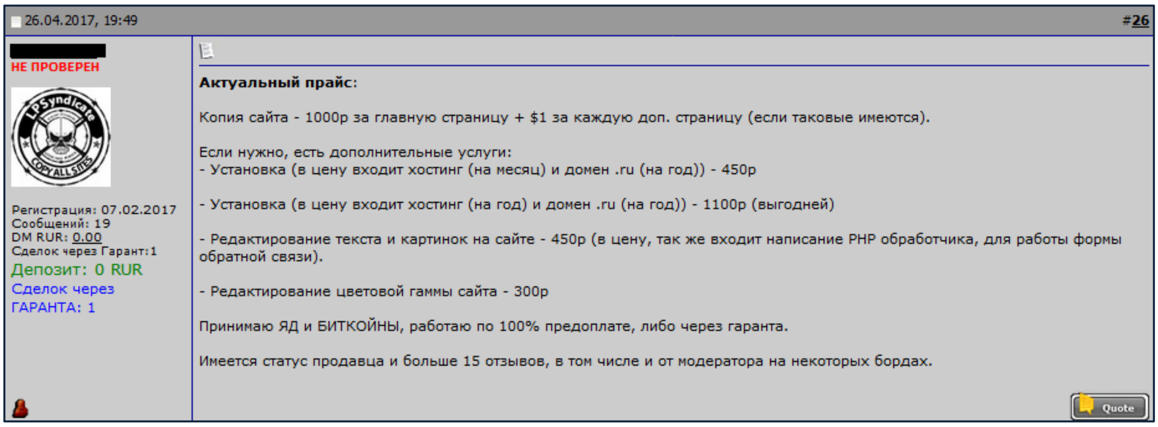
Оплата:

- Работаем по 100% предоплате либо через услуги гаранта форума.
- Принимаем: QIWI | Яндекс. Деньги

Контакты:

- **Почта**: [redacted]
- **Telergram**: telegram.[redacted](ссылку вставить в браузер)
- **Jabber**: [redacted]
- **ICQ**:[redacted]

In April, the vendor posted exact pricing for his services:



26.04.2017, 19:49 #26

[redacted]
НЕ ПРОВЕРЕН

Регистрация: 07.02.2017
Сообщений: 19
DM RUR: 0.00
Сделок через Гарант:1
Депозит: 0 RUR
Сделок через ГАРАНТА: 1

Актуальный прайс:

Копия сайта - 1000р за главную страницу + $1 за каждую доп. страницу (если таковые имеются).

Если нужно, есть дополнительные услуги:
- Установка (в цену входит хостинг (на месяц) и домен .ru (на год)) - 450р

- Установка (в цену входит хостинг (на год) и домен .ru (на год)) - 1100р (выгодней)

- Редактирование текста и картинок на сайте - 450р (в цену, так же входит написание PHP обработчика, для работы формы обратной связи).

- Редактирование цветовой гаммы сайта - 300р

Принимаю ЯД и БИТКОЙНЫ, работаю по 100% предоплате, либо через гаранта.

Имеется статус продавца и больше 15 отзывов, в том числе и от модератора на некоторых бордах.

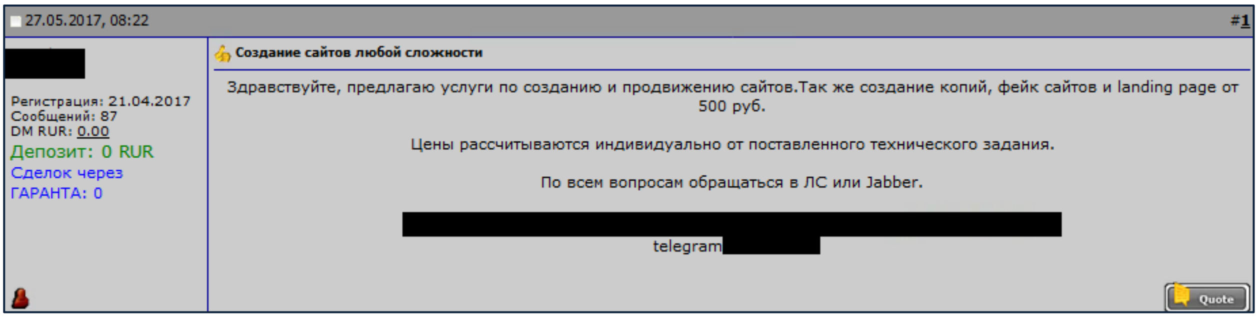
The prices are as following (converted from rubles to dollars):

- Duplication of website – 17$ for the main page + 1$ for every additional page, if exists
- Deployment of the website (including hosting for a **month** and domain .ru for year) – 7.5$
- Deployment of the website (including hosting for a **year** and domain .ru for year) – 18$
- Edition of text and pictures in the website – 7.5$ (the price includes development of PHP scripts for contact forms)
- Edition of color scheme of the website – 5 $

Although his prices are relative very low, he has more than ten very positive feedbacks in different communities.

Vendor12

Another vendor, began offering his services recently, in May 2017:


27.05.2017, 08:22

#1

[redacted]

Регистрация: 21.04.2017
Сообщений: 87
DM RUR: 0.00
Депозит: 0 RUR
Сделок через
ГАРАНТА: 0

Создание сайтов любой сложности

Здравствуйте, предлагаю услуги по созданию и продвижению сайтов.Так же создание копий, фейк сайтов и landing page от 500 руб.

Цены рассчитываются индивидуально от поставленного технического задания.

По всем вопросам обращаться в ЛС или Jabber.

[redacted]

telegram[redacted]

In conversation with the vendor, it seems that he develops the fake websites on relatively average prices, about 45$ for banking login fake, and about 25 $ for adding another page for credit cards grabbing:

ClearSky: I'm regarding the fakes

Vendor12: I am hearing you

ClearSky: I want to ask about the pricing for relatively simple fake

Vendor12: fake of what?
Vendor12: describe please

ClearSky: bank login
*ClearSky: like online. ***bank.***

Vendor12: what functionality should be?
Vendor12: 2500

ClearSky: and if I add to the fake another page (second stage) for (collecting -Clearsky) cc + cvv … how it changes the price?

Vendor12: about 1200-1500

ClearSky: are you duplicating or developing?

Vendor12: developing

ClearSky: do you have some examples of you works? Or feedback?

Vendor12: has a lot of examples of the work. The last one is http://c2c.myjino.ru – cards logs saving
Vendor12: you can enter cards info on the site and press "transfer"

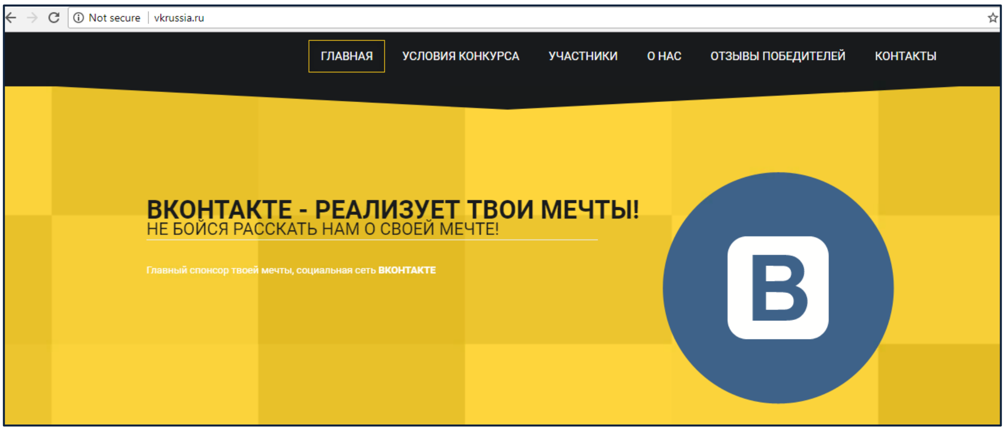
ClearSky: and banking fakes examples?

Vendor12: don't have banking fakes. But will do quickly and with high quality

Vendor13

This vendor began offering his services in June 2017, from offering ready fake set for Vkontakte including scam scheme that assists stealing VK accounts; the set includes resembling domain name (vkrussia.ru), the fake website and promotional short movie made for this specific domain name.

The fake page:

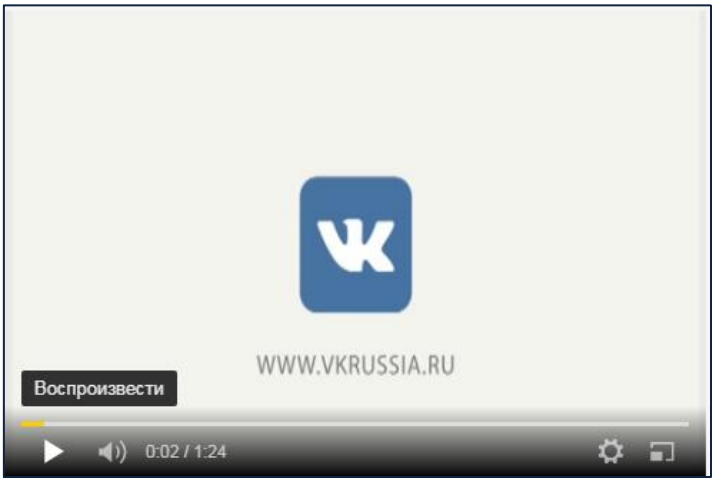


ВКОНТАКТЕ - РЕАЛИЗУЕТ ТВОИ МЕЧТЫ!

НЕ БОЙСЯ РАССКАТЬ НАМ О СВОЕЙ МЕЧТЕ!

Главный спонсор твоей мечты, социальная сеть ВКОНТАКТЕ

The promotional movie:



In parallel, he began offering several other fakes that are ready, and development of new fakes.

He specified the pricing for his ready fakes (converted to dollars):

Fake for Vkontakte (including the domain vkhistory.ru) – 33$
Fake for Facebook (including the domain fb-story.ru) – 35$
Fake for Odnoklassniki (including the domain ok-mystory.ru) – 35$
Fake for Instagram (including the domain theinstagra.ru) – 35$
Fake for Mail.ru, Gmail.com,Rambler.ru,Yandex.ru – 5$
Fake for Vk – 7$

Direct conversation with the vendor helped us to understand more about him and his work. He is a front-end developer, and seems to be a professional one. The most interesting thing from the conversation from his is the fact that he doesn't know how much to ask for his work:

ClearSky: I want to ask about pricing for fakes
ClearSky: fake for bank login? (Not RU)

Vendor13: do you have terms of reference?

Vendor13: If it just a fake of login page, so I think, it will not be a problem

ClearSky: online.***bank.**

ClearSky: like this for example

Vendor13: Fake of this page? You need to save entered usr id and pass, right? What should happen after the details are entered? Where should the victim be forwarded?

Vendor13: It is possible to forward the victim to the main page of the original

ClearSky: yes fake…and to forward to the original

ClearSky: what will be the price?

Vendor13: I don't have an idea

ClearSky: are you duplicating or developing from scratch?

Vendor13: mostly, I download via wget, and adjust it to the original

Vendor13: Is there any difference whether the page is developed from scratch or duplicated, if the result in both will be the same?

ClearSky: the duplicated are in many cases exposed quickly

ClearSky: and are being blocked in Chrome

Vendor13: Truly, I'm not aware of this

Vendor13: Previously, we have used intermediate domains between the fake and the phishing mail

Vendor13: and after some time just changing the intermediate domain

ClearSky: у вас есть примеры рабом?

Vendor13: Only above- mentioned autosportkbr.ru/facebook

autosportkbr.ru/odnoklassniki

ClearSky: so what will be the price for online.***bank.co.*** ?

Vendor13: Don't have an idea. The same 2000 are acceptable to you?

ClearSky: and if I add to the fake another page (second stage) for CC +CVV… how it changes the price?

ClearSky: i.e. page that doesn't exist in original

ClearSky: you need to develop this page almost from scratch, similar to the design of first page

Vendor13: Do you have some preferences on the design?

Vendor13: to show 404, or something else?

ClearSky: after the second page? Possible 404

Vendor13: See, so it looks like – in the beginning pass and login is entered, afterwards they are forwarded to page of CC + CVV grabbing and then 404, right?

ClearSky: yes

Vendor13: 3000 suits you?

ClearSky: for everything? Think yes

ClearSky: you are a developer? Or just make basic fakes?

Vendor13: I mostly work only on front end

Vendor14

Another vendor began offering the services on April 2017, as all over worker who offered variety of services, including fakes that consists one page, as he posted for 25$. He mentions that he has knowledge in HTML and in CSS. Apart of fakes, he offers his services working with VPS linux, installation of CMS, Joomla and OpenCart and registration in any services needed. It seems that this vendor is an example of all over worker who has basic knowledge in many areas but is not a real specialist in any area.

ClearSky: I'm regarding the fakes
Vendor14: talk
ClearSky: I want to know the pricing for relatively simple fake *ClearSky: for bank login*
Vendor14: beginning at 30$
Vendor14: which country?
*ClearSky: online.***bank.***
Vendor14: what data to grab?
ClearSky: user id + pass
Vendor14: it will cost 50
ClearSky: are you duplicating or developing?
Vendor14: developing

Vendor15

There is another verified vendor, Vendor15 who introduced his services on January 2017, and he is active in several Russian speaking communities, but also posts in English – to attract English speaking clients (spelling mistakes are in the source).

The main services he provides is complete impersonation of corporate websites:

> *Dear Friends I'm happy to introduce the developement service of corporate design, drop projects, web shops, fakes, landing pages, websites and etc.*
>
> *Current prices (turnkey solution):*
>
> *Drop project for cashing - $1000*
> *Drop Project for stuff - $800*
> *Development time range 7-9 days.*
> *What do you get:*
> *Complete website with modern hq corporate design, Content Management System (CMS) of your website Employment agreement, application form and other required documents.*
> *Full step by step instruction, which allows you to execute a correspondence with "hired employees" without fluent knowledge of english language.*
> *Company legend, hosting and domain.*
>
> *English speakers always welcomed.*
> *Payment on Bitcoin or webmoney*

As well, he develops web shops, mostly for illegal goods selling (servers, credit cards, banking accounts, etc.) and imitates fake company activity and reputation in google (kind of SEO).