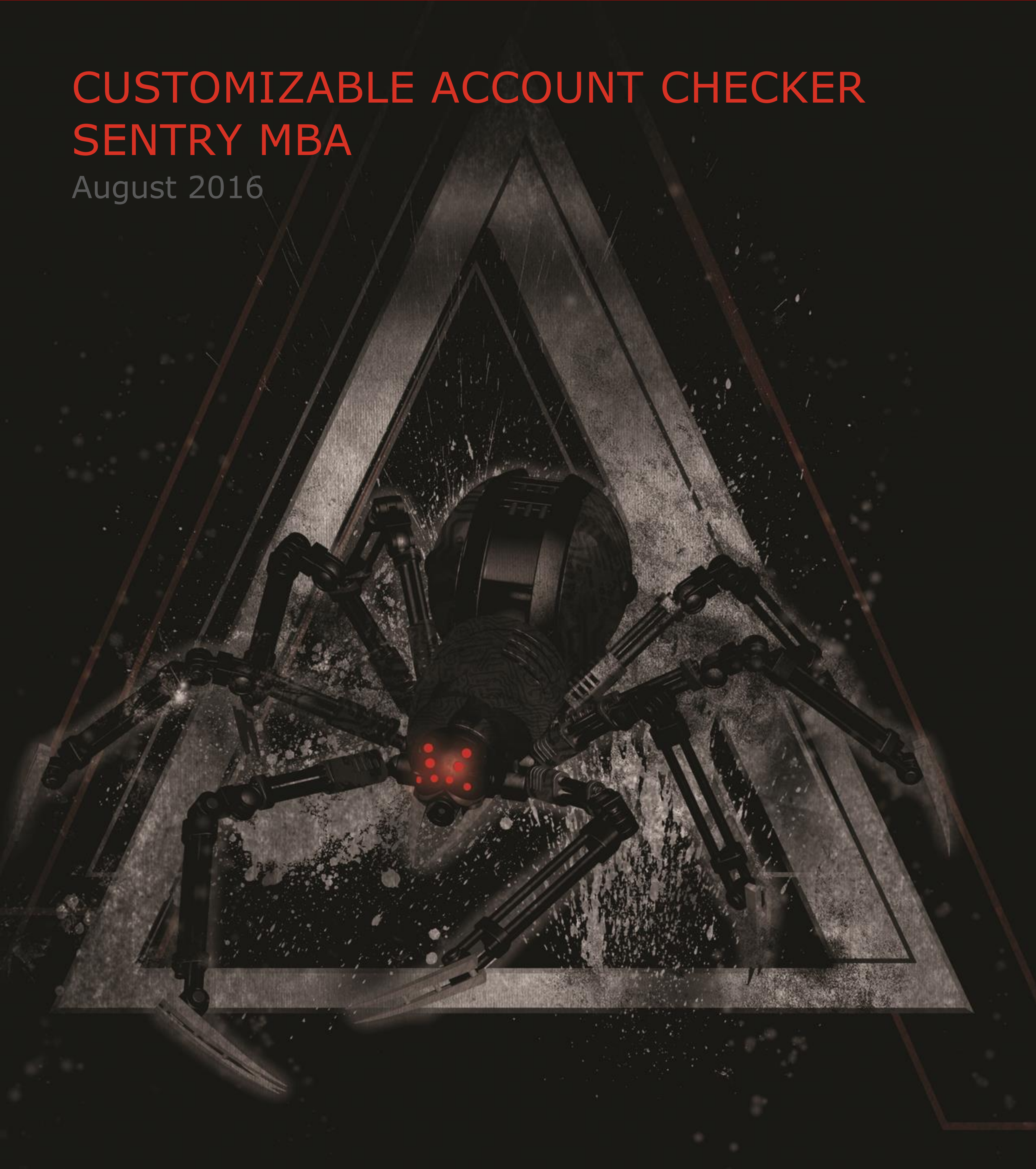
FraudAction™ Knowledge Delivery

RSA

CUSTOMIZABLE ACCOUNT CHECKER SENTRY MBA

August 2016

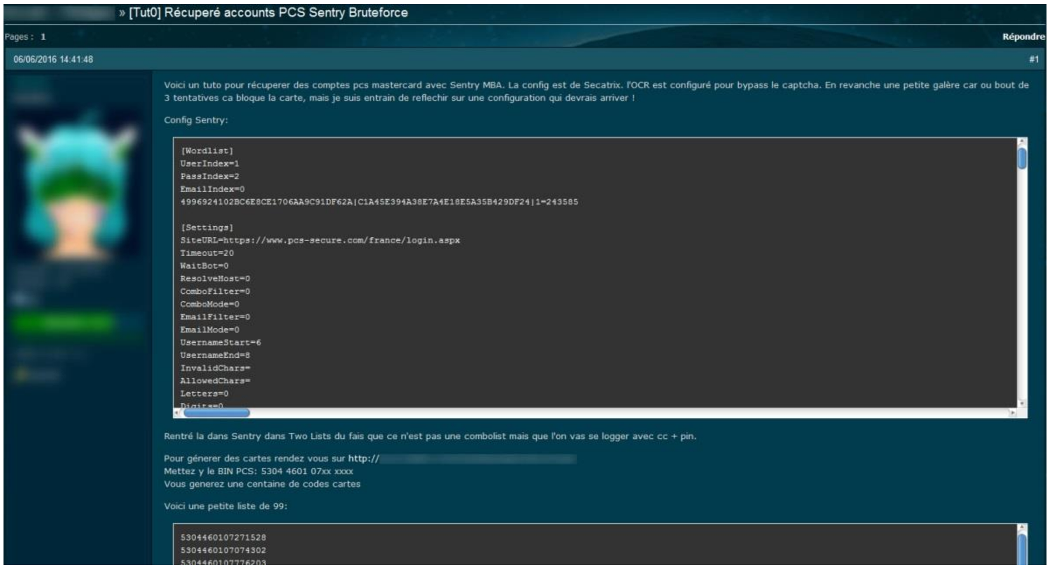


SENTRY MBA

RSA FraudAction analysts have traced a modular and customizable account checking system that is offered openly and at no cost both in the underground and on the open web. Named Sentry MBA, and although this software is at least 2 years old, it has recently been gaining momentum and appears to hold wide interest in the fraud community. The automated system allows a fraudster to check multiple compromised accounts, to customize the list of targeted entities, and to tailor the way each site is approached and checked. In essence, this is a form of brute-force attack software that attempts to log in to multiple accounts with a long list of compromised credentials.

Figure 1: Sentry MBA version 2.0 logo

Figure 2: Sentry MBA tutorial offered in a French underground forum



[redacted] » [Tut0] Récuperé accounts PCS Sentry Bruteforce

Pages : 1 Répondre

06/06/2016 14:41:48 #1

Voici un tuto pour récuperer des comptes pcs mastercard avec Sentry MBA. La config est de Secatrix. l'OCR est configuré pour bypass le captcha. En revanche une petite galère car ou bout de 3 tentatives ca bloque la carte, mais je suis entrain de reflechir sur une configuration qui devrais arriver !

Config Sentry:

```
[Wordlist]
UserIndex=1
PassIndex=2
EmailIndex=0
4996924102BC6E8CE1706AA9C91DF62A|C1A45E394A38E7A4E18E5A35B429DF24|1=243585

[Settings]
SiteURL=https://www.pcs-secure.com/france/login.aspx
Timeout=20
WaitBot=0
ResolveHost=0
ComboFilter=0
ComboMode=0
EmailFilter=0
EmailMode=0
UsernameStart=6
UsernameEnd=8
InvalidChars=
AllowedChars=
Letters=0
Digits=0
```

Rentré la dans Sentry dans Two Lists du fais que ce n'est pas une combolist mais que l'on vas se logger avec cc + pin.

Pour génerer des cartes rendez vous sur http://[redacted]
Mettez y le BIN PCS: 5304 4601 07xx xxxx
Vous generez une centaine de codes cartes

Voici une petite liste de 99:

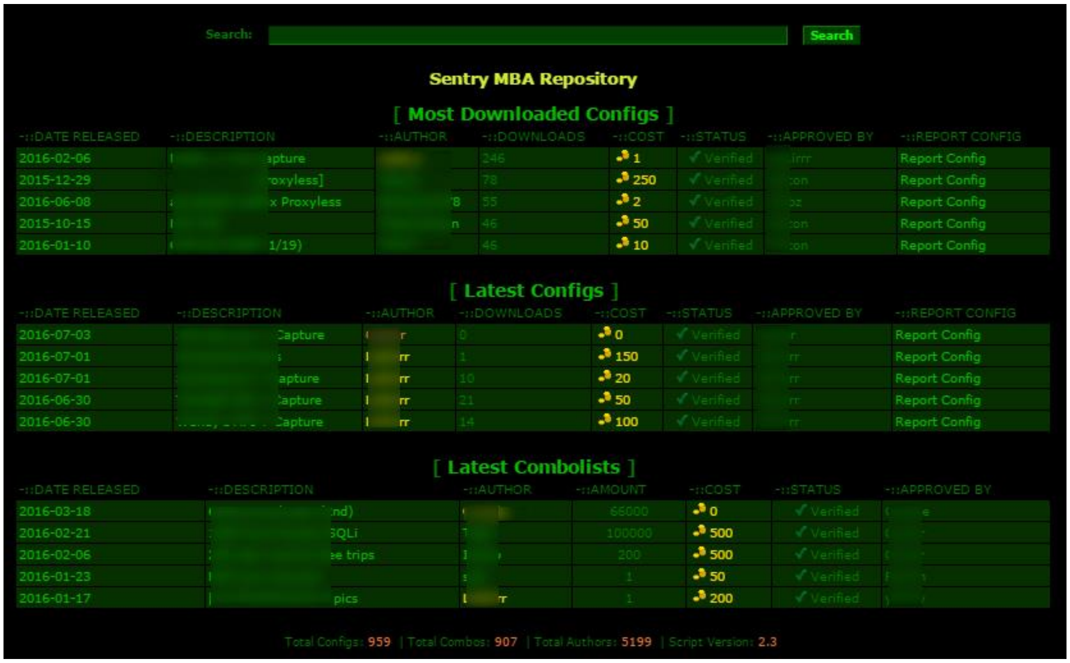
```
5304460107271528
5304460107074302
5304460107776203
```

The system is modular, and works with configuration files that define the target and the exact approach for the attempted login. An example of a versatile module offered for Sentry MBA is an OCR image recognition module that can read the image presented in a CAPTCHA security challenge, using an open source module named Tesseract, and leveraging a number of authorization service databases (including Strongbox) in order to automate getting past the protection. Other modules available in the Sentry MBA suite provide support for JavaScript and for Ajax to help handle more complex sites and sophisticated multiple step login mechanisms.

While the main Sentry MBA framework is available for free in numerous sites and forums, the configuration files are offered for sale as a service (FaaS) in forums and underground marketplaces, and a few ready-made configuration files are offered for free.

The Sentry.mba website offers a repository for the software as well as config files and combo lists that target major popular retail brands, media services and such. One must first register with the site before being able to upload or download any of the files. In order to carry out transactions in the site, one must purchase Sentry MBA 'Gold' internal currency.

Figure 3: Sentry MBA repository site offering customized config files that target major retail brands



Sentry MBA Repository

[Most Downloaded Configs]

-::DATE RELEASED	-::DESCRIPTION	-::AUTHOR	-::DOWNLOADS	-::COST	-::STATUS	-::APPROVED BY	-::REPORT CONFIG
2016-02-06	[redacted] apture	[redacted]	246	1	✓ Verified	[redacted] irrr	Report Config
2015-12-29	[redacted] roxyless]	[redacted]	78	250	✓ Verified	[redacted] con	Report Config
2016-06-08	[redacted] x Proxyless	[redacted] 8	55	2	✓ Verified	[redacted] oz	Report Config
2015-10-15	[redacted]	[redacted] n	46	50	✓ Verified	[redacted] con	Report Config
2016-01-10	[redacted] 1/19)	[redacted]	46	10	✓ Verified	[redacted] con	Report Config

[Latest Configs]

-::DATE RELEASED	-::DESCRIPTION	-::AUTHOR	-::DOWNLOADS	-::COST	-::STATUS	-::APPROVED BY	-::REPORT CONFIG
2016-07-03	[redacted] Capture	[redacted] r	0	0	✓ Verified	[redacted] r	Report Config
2016-07-01	[redacted] s	[redacted] rr	1	150	✓ Verified	[redacted] rr	Report Config
2016-07-01	[redacted] apture	[redacted] rr	10	20	✓ Verified	[redacted] rr	Report Config
2016-06-30	[redacted] Capture	[redacted] rr	21	50	✓ Verified	[redacted] rr	Report Config
2016-06-30	[redacted] Capture	[redacted] rr	14	100	✓ Verified	[redacted] rr	Report Config

[Latest Combolists]

-::DATE RELEASED	-::DESCRIPTION	-::AUTHOR	-::AMOUNT	-::COST	-::STATUS	-::APPROVED BY
2016-03-18	[redacted] nd)	[redacted]	66000	0	✓ Verified	[redacted]
2016-02-21	[redacted] SQLi	[redacted]	100000	500	✓ Verified	[redacted]
2016-02-06	[redacted] e trips	[redacted]	200	500	✓ Verified	[redacted]
2016-01-23	[redacted]	[redacted]	1	50	✓ Verified	[redacted]
2016-01-17	[redacted] pics	[redacted] r	1	200	✓ Verified	[redacted]

Total Configs: 959 | Total Combos: 907 | Total Authors: 5199 | Script Version: 2.3

Typical prices for Sentry MBA config files

Brand/Business type	Config Type	Sentry MBA Gold	Dollars
Major retail chain	API Proxyless	250	$2.08
Major retail chain	plain config	25	$0.21
Major fast-food chain	API	50	$0.42
Media download site	Proxyless	15	$0.12
Social media site	Proxyless	15	$0.12
Gaming site	gaming	1999	$16.66
Stock photos site	proxyless	250	$2.08

** $1.00 = 120 'Gold'

In addition to the main resource website, Sentry MBA appears to have wide support in fraud communities on Facebook and in the underground. One can easily find config files and combo lists offered for sale, as well as a few 'freebies' in many forums and communities around the world - our analysts found examples in French, Arabic, Spanish, Russian, and Chinese speaking forums and groups. Questions and discussions seen in Sentry MBA focused community groups on Facebook provide real-time feedback to the developers of the software, which may explain the fairly frequent version updates and fixes that have been released over the last 2 years.

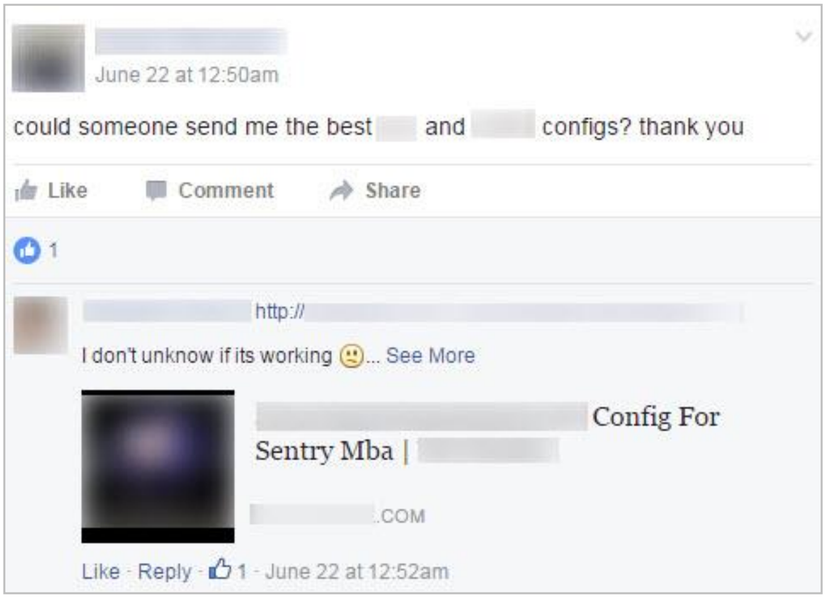


Figure 4: Facebook entry – looking for Sentry MBA config files

[redacted]
June 22 at 12:50am

could someone send me the best [redacted] and [redacted] configs? thank you

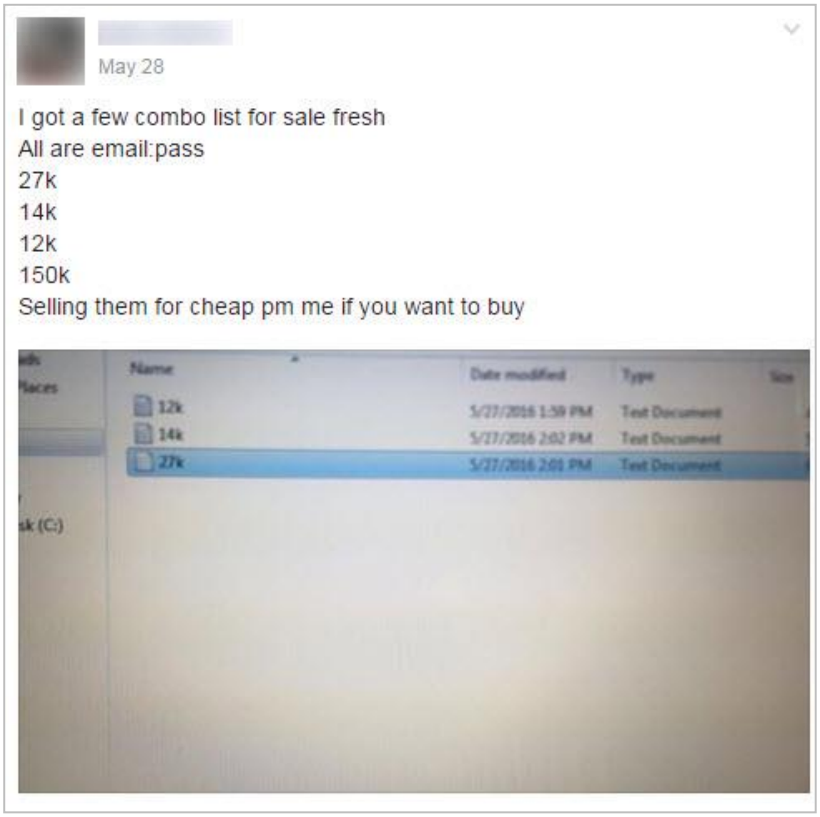
[redacted] http:// [redacted]
I don't unknow if its working 🙁... See More

[redacted] Config For Sentry Mba | [redacted]

[redacted].COM

· June 22 at 12:52am

Figure 5: Facebook entry – fresh combo list for sale

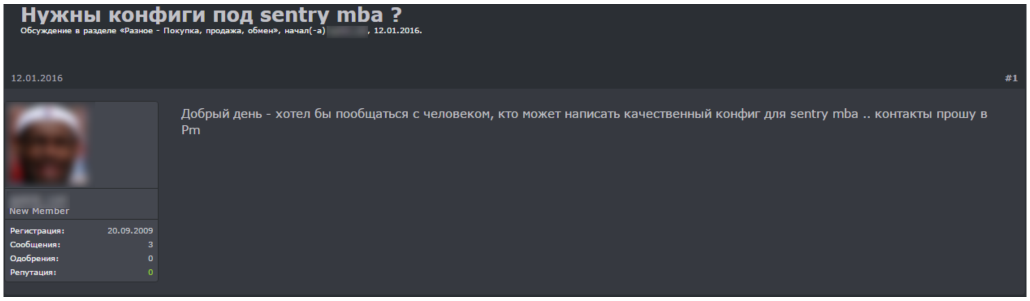


[redacted]
May 28

I got a few combo list for sale fresh
All are email:pass
27k
14k
12k
150k
Selling them for cheap pm me if you want to buy

Name	Date modified	Type
12k	5/27/2016 1:59 PM	Text Document
14k	5/27/2016 2:02 PM	Text Document
27k	5/27/2016 2:01 PM	Text Document

Figure 6: Russian speaking underground forum requesting Sentry MBA config files



Нужны конфиги под sentry mba ?
Обсуждение в разделе «Разное - Покупка, продажа, обмен», начал(-а) [redacted], 12.01.2016.

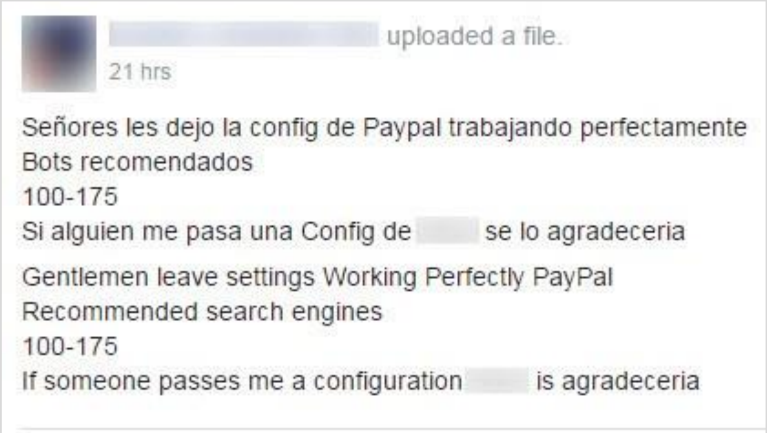
12.01.2016 #1

Добрый день - хотел бы пообщаться с человеком, кто может написать качественный конфиг для sentry mba .. контакты прошу в Pm

[redacted]
New Member

Регистрация:	20.09.2009
Сообщения:	3
Одобрения:	0
Репутация:	0

Figure 7: Spanish speaking Facebook entry - Sentry MBA config files

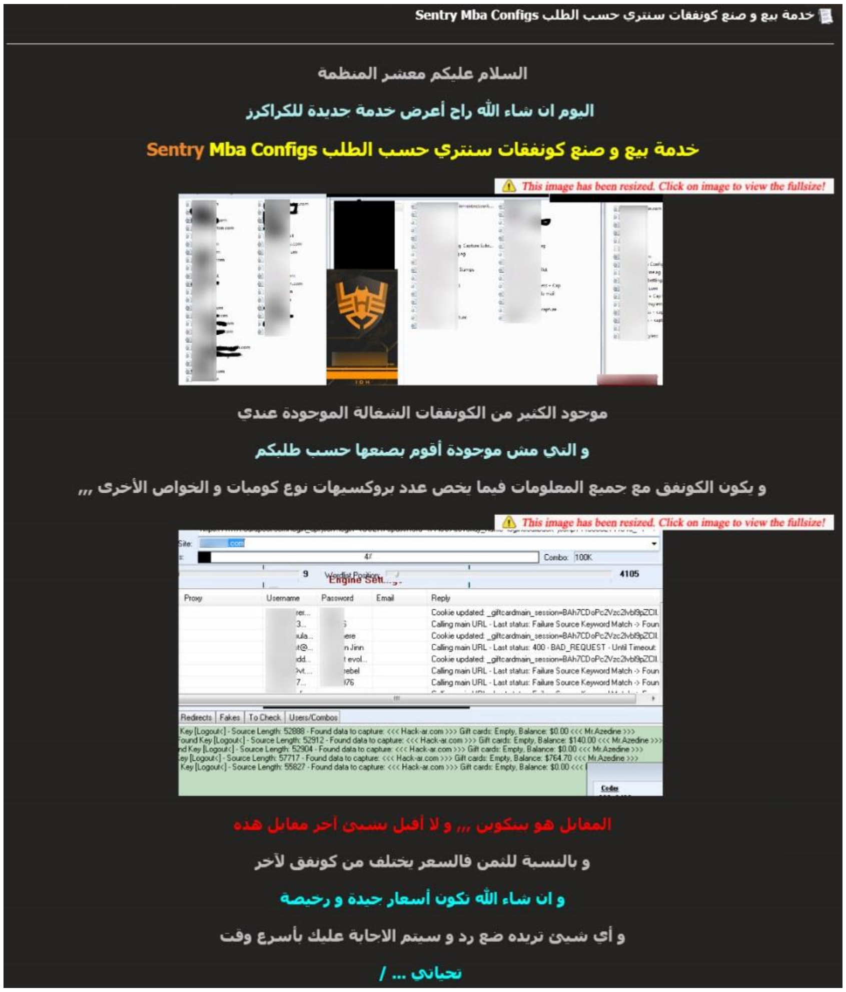


[redacted] uploaded a file.
21 hrs

Señores les dejo la config de Paypal trabajando perfectamente
Bots recomendados
100-175
Si alguien me pasa una Config de [redacted] se lo agradeceria

Gentlemen leave settings Working Perfectly PayPal
Recommended search engines
100-175
If someone passes me a configuration [redacted] is agradeceria

Figure 8: Arabic speaking underground forum offering Sentry MBA config files



خدمة بيع و صنع كونفقات سنتري حسب الطلب Sentry Mba Configs

السلام عليكم معشر المنظمة

اليوم ان شاء الله راح أعرض خدمة جديدة للكراكرز

خدمة بيع و صنع كونفقات سنتري حسب الطلب Sentry Mba Configs

This image has been resized. Click on image to view the fullsize!

موجود الكثير من الكونفقات الشغالة الموجودة عندي

و التي مش موجودة أقوم بصنعها حسب طلبكم

و يكون الكونفق مع جميع المعلومات فيما يخص عدد بروكسيهات نوع كومبات و الخواص الأخرى ,,,

This image has been resized. Click on image to view the fullsize!

Site: [redacted].com

47 Combo: 100K

9 Wordlist Position: 4105

Engine Sett...

Proxy	Username	Password	Email	Reply
	[redacted]	[redacted]		Cookie updated: _giftcardmain_session=BAh7CDoPc2Vzc2lvbl9pZCII.
	[redacted]	[redacted]		Calling main URL - Last status: Failure Source Keyword Match -> Foun
	[redacted]	[redacted]		Cookie updated: _giftcardmain_session=BAh7CDoPc2Vzc2lvbl9pZCII.
	[redacted]	[redacted]		Calling main URL - Last status: 400 - BAD_REQUEST - Until Timeout:
	[redacted]	[redacted]		Cookie updated: _giftcardmain_session=BAh7CDoPc2Vzc2lvbl9pZCII.
	[redacted]	[redacted]		Calling main URL - Last status: Failure Source Keyword Match -> Foun
	[redacted]	[redacted]		Calling main URL - Last status: Failure Source Keyword Match -> Foun

```
Key [Logout<] - Source Length: 52888 - Found data to capture: <<< Hack-ar.com >>> Gift cards: Empty, Balance: $0.00 <<< Mr.Azedine >>>
Found Key [Logout<] - Source Length: 52912 - Found data to capture: <<< Hack-ar.com >>> Gift cards: Empty, Balance: $140.00 <<< Mr.Azedine >>>
nd Key [Logout<] - Source Length: 52904 - Found data to capture: <<< Hack-ar.com >>> Gift cards: Empty, Balance: $0.00 <<< Mr.Azedine >>>
ey [Logout<] - Source Length: 57717 - Found data to capture: <<< Hack-ar.com >>> Gift cards: Empty, Balance: $764.70 <<< Mr.Azedine >>>
Key [Logout<] - Source Length: 55827 - Found data to capture: <<< Hack-ar.com >>> Gift cards: Empty, Balance: $0.00 <<<
```

المقابل هو بتكوين ,,, و لا أقبل بشيء آخر مقابل هذه

و بالنسبة للثمن فالسعر يختلف من كونفق لآخر

و ان شاء الله تكون أسعار جيدة و رخيصة

و أي شيء تريده ضع رد و سيتم الاجابة عليك بأسرع وقت

تحياتي ... /

Advertised Sentry MBA Features

(condensed from the Sentry MBA ReadMe document)

- *Supports Ajax*
- *Full OCR support - Supports Fixed Captcha OCR sites (for example, sites that use Strongbox – database included) by user configurable database, "Acquire Images" engine allows updating the database for fixed captcha sites. Ability to train Tesseract for specific fonts.*
- *Supports HTTPS and SOCKS 4A/5*
- *Advanced configuration of all the engine stages using special variables*
- *Fully configurable Keyword Capture (useful for premium account details) and advanced special Keyword Matching*
- *Supports configurable Form JavaScript Redirect (useful to reach premium account page)*
- *Supports multiple additional form redirects, (to call additional URLs and capture keys from multiple pages)*
- *Supports advanced custom Parsing Code*
- *Advanced Proxy Analyzer - special cleaning and filtering functions, including proxy filtering by IpFilter (IpFilter tweaked for Sentry is included)*
- *Other unique features that you must discover by yourself*

Prerequisites

- Sentry MBA software
- Config file – [*.ini] file containing specific parameters for your target site
- Combo list - list of compromised emails/passwords
- Proxy list – list of proxy addresses used to be used to disguise the origin of the attack

Method – Using Sentry MBA

1. Download and install the Sentry MBA package
2. Import .ini config: Settings -> General -> Load Settings from Snap Shot (*.ini)
3. Import the *Proxy list*: *Lists* > *Proxylist*
4. Import a *Combo list*:
5. Go to *Progression*, and set the number of bots (set between 15-30 bots so the Proxy will not ban you for too high a rate)
6. Click *Start*
7. Click *Start a Bruteforce Session* in the popup dialog, select *Use the Progression Position*.

ABOUT RSA

RSA's solutions help organizations execute advanced cyber defense strategies that reduce the risks of operating in a digital world. Through visibility and analytics, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud, and cybercrime. For more information on RSA, please visit www.rsa.com.

ABOUT RSA FRAUDACTION

RSA FraudAction is a managed threat intelligence service which provides global organizations with 24x7 protection and shutdown against phishing, malware, rogue mobile apps and other cyber attacks that impact their business. Supported by 150 analysts in RSA's Anti-Fraud Command Center, the RSA FraudAction service analyzes millions of potential threats every day and has enabled the shutdown of more than one million cyber attacks.