peace_of_mind

View of the analyst

Cyber identity `peace_of_mind` (also Peace and `peace@rows.io`) responsible for the sale of LinkedIn, Myspace, Tumblr and Vk databases, among others, also corresponds to the group connected to the sale of *exploit kits* on the Tor network. Another identifier potentially connected to this group is the Jabber account `tessa88@exploit.im`.

Figure 1. Peace's Shop Avatar.

The method used to spread the compromised databases is based on their promotion via the bitcoin marketplace platform TheRealDeal, which is solely accessible via a hidden service in Tor and which has made at least 59 sales at a value of at least 58,5264 BTC (40,617 dollars, by conversion). Likewise, the alleged perpetrators use different Jabber servers are contact points for instant messaging, in addition to offering the possibility to use PGP for encrypted communication.

Table I. General information about the identified avatars.

Identifiers:	`peace_of_mind`; `peace`; `tessa88 (unconfirmed);`
Signed:	«Shady dark web data dealer»
Nationality:	[N/F]
Languages:	English (not native)
Known affiliations:	[N/F]
Skills:	Exploit kits creation Filtered database sales

Detail

The username `peace_of_mind` first appeared on the TheRealDeal marketplace platform, which is only accessible via Tor, which is connected to the lookbook.nu information leak. Among the most significant activities, one can highlight the sale of leaks in relation to high-level platforms such as LinkedIn, Myspace, Tumblr and Vk, adding up to a total of more than 800 million leaked credentials. This used has received 47 positive reviews accrediting them as a trusted vendor within the platform and as of June 8th, 2016, it uses an image with the logo of the FBI as its profile avatar. On this same date, motivated by the update of the TheRealDeal platform, this user also created a shop called Peace's Shop within the same marketplace.

For an avatar, it uses a modified image of a wooden arrow on a beach that has been retouched to include the text `PEACE OF MIND` on it. The user also uses as an image of the Krebs on Security blog as a banner. These images contain the same metadata since the platform does not eliminate it: `CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90.` The GD book store is used by applications such as Widelmage to manipulate images.

Additional information

The cyber identity seems to be connected to the TheRealDeal marketplace at the PGP key `08E17DFB` (RSA of 4096 bits), created on the 14th of February, 2016 and with no expiry date. The User-ID for the key presents the following information:

```
peace (TRD Admin http://trdealmgn4uvm42g.onion) peace@rows.io
```

In such commentary the name `peace` appears, the mention to `TRD Admin` (TheRealDeal initials) and the domain .onion where said marketplace is located (`http://trdealmgn4uvm42g.onion`). On the other hand, the public key seems to be associated with `peace@rows.io` which corresponds to a Jabber account.

Investigation into `peace@rows.io` through Tor network searches has enabled identification in the `pekitb7z6owuvoko.onion` domain of the same account associated with the sale of an exploit kit with seven CVEs and at least two private exploits. On said web page there appear screenshots over a control panel that, on a map, represents as an example the victims of Ukraine, Russia and Chile. Said screenshots were taken by the `mate-screenshot` tool that is part of the MATE desktop environment (based on GNOME 2) and whose development is borne by Linux Mint and Ubuntu.

According to the page content, the perpetrators announced the sale of the exploit kit in some semi-private forums, though they also mention that it can be acquired at a URL of TheRealDeal that, at the time of consultation, was not available. Similarly, it has been possible to determine that the offering of these services is prior to the database sale since, according to the headlines on the consulted web page, housed in an nginx server, it has not been modified since January 4th, 2016.

On the other hand, the official communication regarding the Myspace leak issued by LeakedSource, a platform dedicated to leaked monitoring databases, points to the `tessa88@exploit.im`[1] Jabber account as the origin of the leak, in addition to the making a reference in plural («them») to the cyber identity responsible for the attack. On June 8th, 2016, this same platform announced for the first time that it had included a database of 32 million Twitter users in its monitoring tool[2]. In the statement issued via its blog, it maintains that the leak was privately facilitated once again by the `tessa88@exploit.im` account. This is the first leak for which there is proof that it can be attributed to said Jabber account without it having been involved in the TheRealDeal marketplace sale, as had occurred with Vk, Myspace and LinkedIn.

It has not been possible to confirm the hypothesis that the cyber identities `tessa88@exploit.im` and `peace_of_mind` pertain to the same group beyond the coincidence of the leaked databases, and so we could be dealing with figures dedicated to the resale of credentials. If this relation could be confirmed, the possibility that this is an organised group gains strength, keeping in mind that the first person plural has been used up to twelve times on the page `pekitb7z6owuvoko.onion.`

[1] Exploit.im is a messaging platform of Russian origin that currently operates from a French server (specifically from Nord-Pas-de-Calais) and whose data logger uses a post code address whose validity has not been verified. Neither the address nor the post code corresponding to the information has been found within the metropolitan area of Moscow. On the other hand, messages sent between users of the provider are encrypted end to end by default.

[2] LeakedSource, «LeakedSource Analysis of Twitter.com Leak», LeakedSource. [Online]. Available at: https://www.leakedsource.com/blog/twitter. [Accessed: 13-jun-2016].

Table II. Gathering of identified evidence.

Date consult	Source type	Description	EF[3]
2016/06/13	*Market underground*	Identification of the `peace_of_mind` username in the TheRealDeal marketplace [1].	B1
2016/06/13	PGP Key	Identifier of the PGP key associated with the `peace_of_mind` user in the TheRealDeal marketplace [2]: `08E17DFB`.	C1
2016/06/13	PGP Key	Additional information associated with the PGP key 08E17DFB: `peace (TRD Admin http://trdealmgn4uvm42g.onion) peace@rows.io` Creation date would correspond to 2016/02/14. Also available at PGP MIT [3].	A1
2016/06/13	Jabber	Sale of an *exploit kit* in a hidden service [4] by `peace@rows.io`. Theoretical data of last modification: 2016/01/04.	C2
2016/06/13	Blog	LeakedSource points to the Jabber account `Tessa88@exploit.im` as the origin of the Myspace [5] and Vk leaks[6].	B2
2016/06/13	Metadata	Use of the `mate-screenshot` tool to perform screenshots [7], [8] and [9].	C2
2016/06/13	*Hidden service*	Location of the sale of the *exploit kit* via TheRealDeal [10].	B2
2016/06/13	*Market underground*	Creation of the shop Peace's Shop within the TheRealDeal marketplace, taking advantage of the web page's update on June 8th [11].	B1
2016/06/13	Blog	LeakedSource points to the Jabber account `Tessa88@exploit.im` as the origin of the new Twitter leak [12].	B2

Both `Tessa88` and `peace_of_mind` or `peace` correspond to names of generic users. The alias `peace_of_mind` is present in up to 30 social networks and four users in different email services, `Tessa88` is present on 33 social networks and three email services and `peace` on 101 platforms and nine email services. The use of generic names is a good operational security practice recommended in underground settings in order to impede account tracking and obtaining identifying information about the attackers, even in the case that the implicated person, by mistake, accidentally leaks information.

Motives

This is an organisation with cybercriminal interests that has tried to monetise both information leaks and exploit kits in marketplaces that use Bitcoin as the payment currency. It cannot be dismissed that said information has previously been used for illicit activities.

The leaks have been concentrated between the months of February and June, 2016, but have not occurred simultaneously in spite of the fact that they are information leaks from the past. The most recent statements have coincided with the highest values for Bitcoin prices in the past two years[4] and during a period of maximum interest by both specialised media and security businesses in database filtering.

[3] According to the International System for Source Evaluation, these are classified according to two variables: source reliability and content credibility. The reliability of a source is scored with one of the following letters: A reliable, B usually reliable, C fairly reliable, D not usually reliable, E unreliable and F cannot be judged. Content credibility is indicated with a number according to the following scale: 1 confirmed, 2 probably true, 3 possibly true, 4 doubtfully true, 5 improbable, 6 cannot be judged.

[4] blockchain.info, «Bitcoin Precio de Mercado (USD)», 13-jun-2016. [Online]. Available at: https://blockchain.info/es/charts/market-price. [Accessed: 13-jun-2016].

As of May 13th, 2016, cyber identity `peace_of_mind` had managed to make 59 sales at a value of at least 58,5264 BTC (40,617 dollars, by conversion). The price of some of his/her products seems fixed in bitcoins given that the quantity does not vary according to its price (Vk.com, Myspace and LinkedIn specifically). For the remaining products, we can observe small variations according to the exchange rate, which suggests that the price is fixed in another currency.

Table III. Sequence of actions confirmed by cyber identity peace_of_mind.

Source	Date[5]	Action	Quantity	Price[6]	Comments	Sales
TheRealDeal	2016/06/13	iMesh filtration	51 million	0.5000 BTC	Fixed in BTC	0
TheRealDeal	2016/06/09	Twitter.com filtration	71 million	0.5000 BTC	Fixed in BTC	4
TheRealDeal	2016/06/05	Vk.com filtration	100 million	1.0000 BTC	Fixed in BTC	8
TheRealDeal	2016/05/26	Myspace filtration	360 million	6.0000 BTC	Fixed in BTC	3
TheRealDeal	2016/05/17	LinkedIn filtration	167 million	2.0000 BTC	Fixed in BTC	11
TheRealDeal	2016/05/12[a]	Tumblr filtration	68 million	0.1473 BTC	--	6
TheRealDeal	2016/05/06[a]	Fling.com filtration	40 million	0.4418 BTC	--	10
TheRealDeal	2016/04/2[m]	Pennsylvania [sic] Voter filtration	N/A	0.0884 BTC	--	3
TheRealDeal	2016/04/14[m]	US Government Data filtration	N/A	0,0736 BTC	--	2
TheRealDeal	2016/03[a]	R2games filtration	22 million	0.2558 BTC	--	3
TheRealDeal	2016/03/18[a]	17 media filtration	30 million	0.2556 BTC	--	6
TheRealDeal	2016/02/23[m]	zepo.in filtration	978 490	0.5112 BTC	--	0
TheRealDeal	2016/03/21[m]	1Ookbook.nu filtration	1.1 million	0.1704 BTC	--	3
pekitb7z6owuvoko.onion	2016/01/04	Exploit Kit sale	N/A	--	--	--

[5] Dates marked with [a] are approximate dates. Dates marked with [m] show the date of the offer's last modification.

[6] Fixed prices in bitcoins as of 13 June 2016, 11:00 UTC+2.