The Ransomware Doctor Without a Cure

research.checkpoint.com/2018/the-ransomware-doctor-without-a-cure/

December 2, 2018

When it comes to ransomware attacks, there is nothing a company hates more than paying the demanded ransom. It is an unexpected fine often caused by a tiny, yet crucial mistake – an unpatched device, an out-of-date product or an innocent human error. It may harm the reputation of the security department, but most of all, it's the idea of paying a significant, though unnecessary, amount of money to a malicious actor. And even then, there is no guarantee the files will actually be recovered. Accordingly, national agencies advise against paying the ransom under any circumstances.

So, once infected, there are essentially three options available to the victim:

- Pay the ransom to the threat actor responsible for locking those files in the first place.
- Find if a key is publicly available for the particular strand of malware and use it to unlock the files.
- Pay someone who claims to be able to unlock the files without paying the ransom.

For those who refuse to be extorted by such ransomware attacks, which is the advice the IT security industry recommends, and if no public key is available, the third option above certainly appeals. And it is here that Check Point Research has discovered a unique and worrying new development in the Ransomware landscape.

Usually IT services that aim to help ransomware victims will explain they can only try and do their best, with no promises made. However, a recently spawned cottage industry rides on the back of ransomware infections by offering desperate victims a way to avoid paying the ransom payment and guarantees to unlock their files for even ransomware that has no public key available – now that's quite a promise!

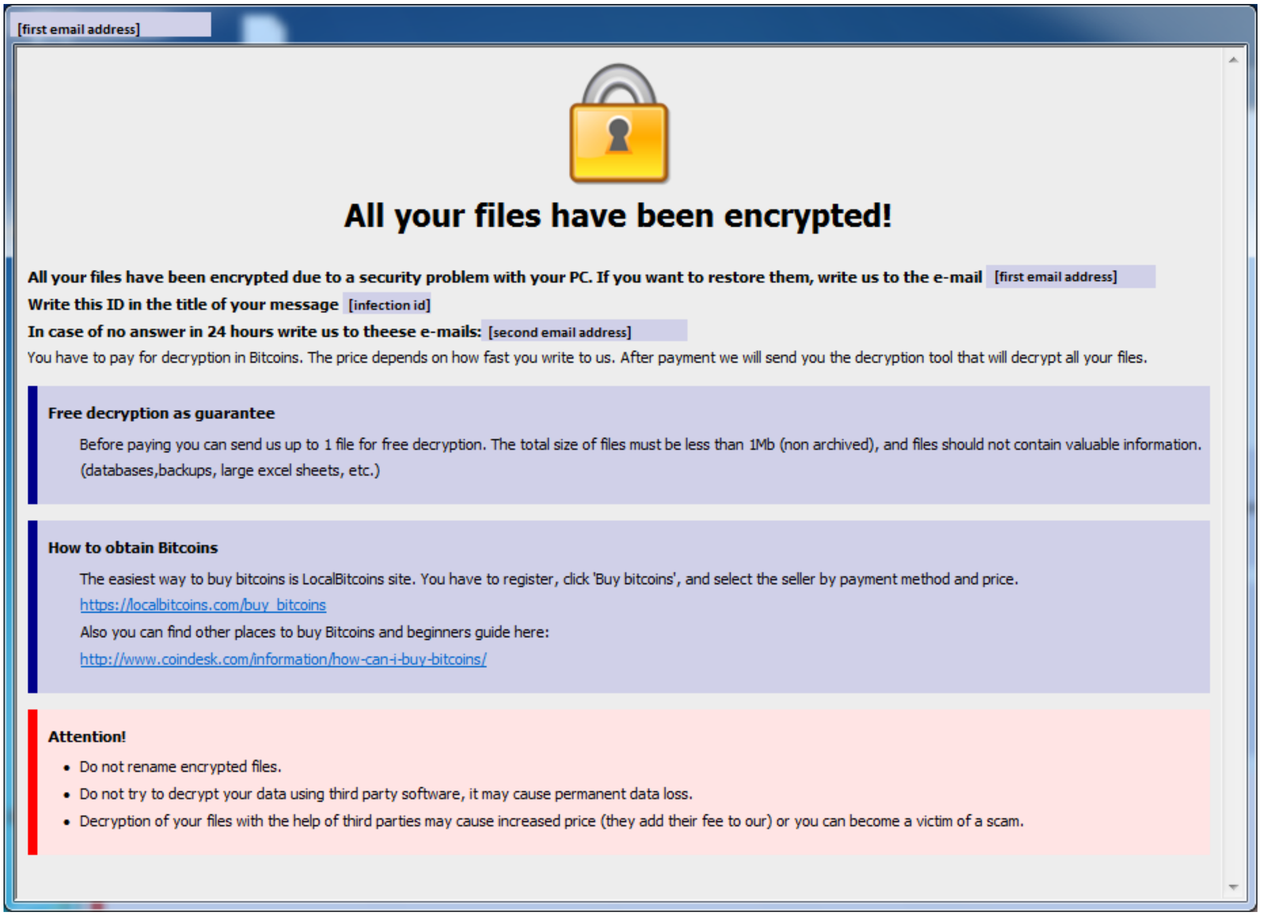
When our team came across a certain service that was making this exact claim, vowing to perform dazzling feats of cyber wizardry to unlock files held captive by the Dharma/Crisis ransomware (for which no decryption key is available), they couldn't help but think something was off, especially when that was the only service that this 'IT consultancy' offers.

After a fascinating investigation, Check Point Research reveals below how a Russian company, named 'Dr. Shifro', claims to legitimately provide file decryption services to ransomware victims, though in fact merely pays the ransomware's author themselves and passes on the cost to the victim – at a massive profit margin.

Furthermore, not only did we uncover the relations and workflow between the Dharma ransomware operators and Dr. Shifro, including the demanded ransom and mediator's profits, but also the possible person behind Dr. Shifro, his whereabouts and his estimated profits.

The Dharma Ransomware

The Crisis ransomware family, also known as Dharma, was first observed in 2016, distributed mainly by spam emails but also via manually hacked RDP access. Upon launch, the malware sets up persistence on a victim's operating system and starts encrypting files with specific extensions that are embedded in the configuration of the ransomware. Fixed, removable and network drives are also affected and, depending on the exact version of the ransomware, some extensions to the name of an encrypted file are added (for example: .dharma, .wallet, .arena, .cobra, .java, .brrr). After the encryption process is finished Dharma then displays a ransom note which provides instructions and two e-mail addresses to contact to obtain the decryption tool.



[first email address]

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail [first email address]
Write this ID in the title of your message [infection id]
In case of no answer in 24 hours write us to theese e-mails: [second email address]
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

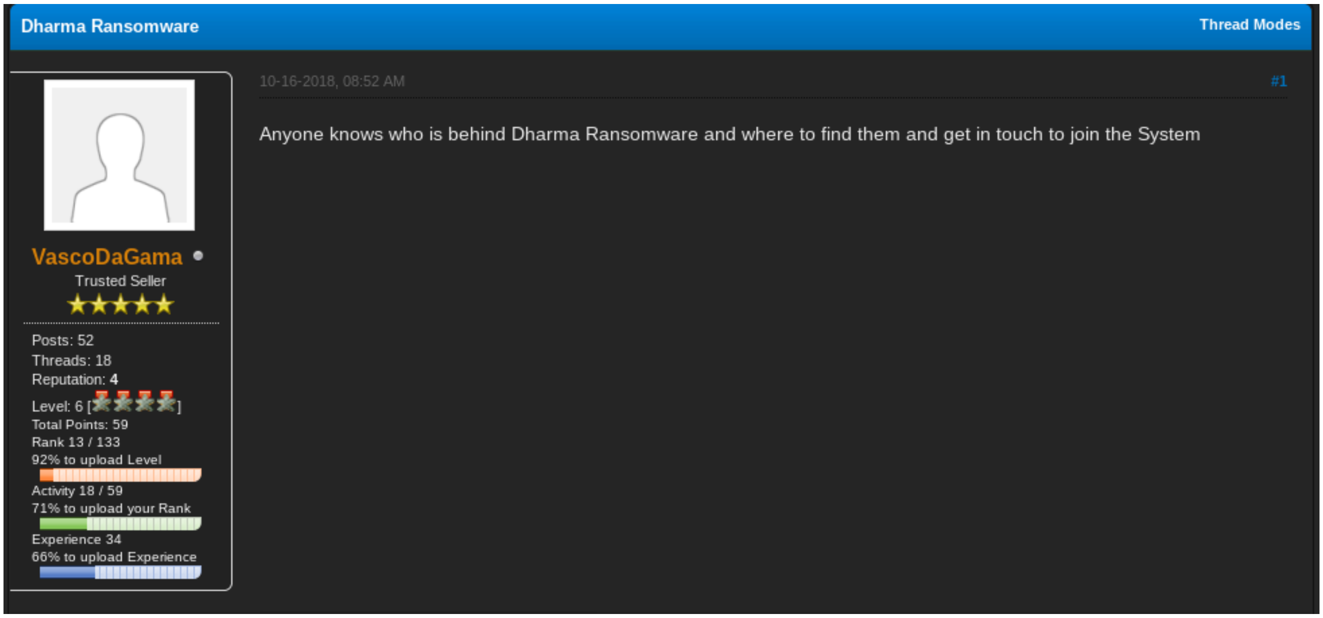
Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Figure 1: Crisis ransom note.

In November 2016 and March 2017 master decryption keys for this ransomware family were released. This allowed security companies to create free decryption tools for this Ransomware.

In autumn 2018, however, we noticed this malware family was still active with new versions that append extensions .arrow, .bip, .gamma, .brrr and others. A quick review of Dharma references on online forums shows that the ransomware is in demand.



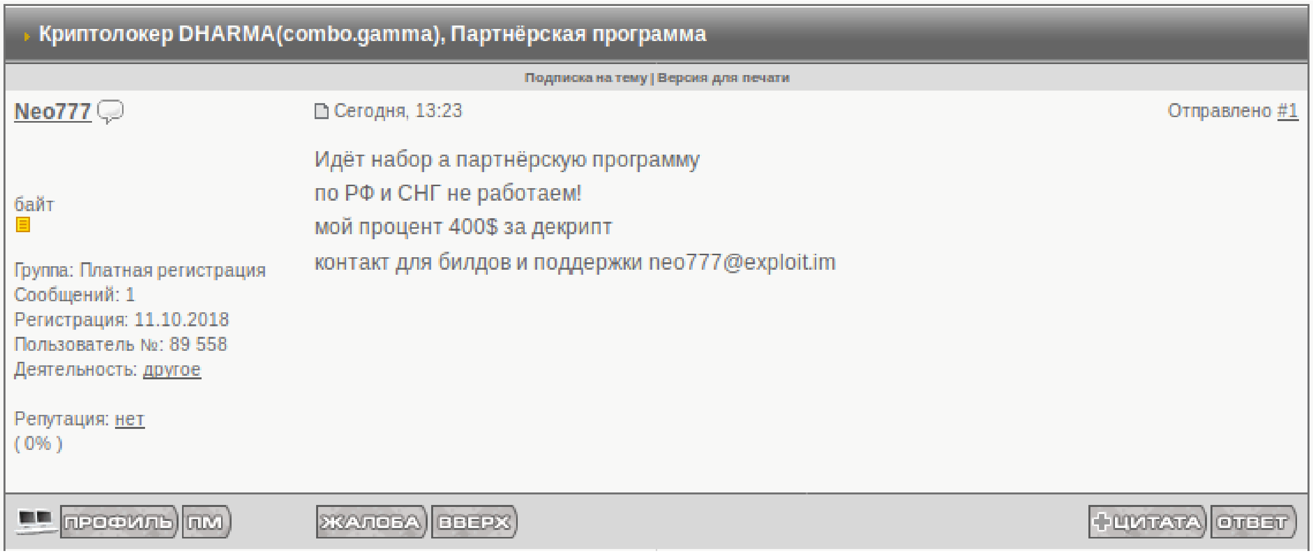
10-16-2018, 08:52 AM #1

Anyone knows who is behind Dharma Ransomware and where to find them and get in touch to join the System

VascoDaGama
Trusted Seller

Posts: 52
Threads: 18
Reputation: 4
Level: 6 []
Total Points: 59
Rank 13 / 133
92% to upload Level
Activity 18 / 59
71% to upload your Rank
Experience 34
66% to upload Experience

Figure 2: A request to join the Dharma ransomware campaign, as posted on the Dark Web.


Криптолокер DHARMA(combo.gamma), Партнёрская программа
Подписка на тему | Версия для печати
ПРОФИЛЬ
ПМ
ЖАЛОБА
ВВЕРХ
ЦИТАТА
ОТВЕТ

Neo777

Сегодня, 13:23 Отправлено #1

Идёт набор а партнёрскую программу
по РФ и СНГ не работаем!
мой процент 400$ за декрипт
контакт для билдов и поддержки neo777@exploit.im

байт

Группа: Платная регистрация
Сообщений: 1
Регистрация: 11.10.2018
Пользователь №: 89 558
Деятельность: другое

Репутация: нет
(0%)

Figure 3: A Dharma ransomware partnership advertisement (*October 18, 2018*). Translation: *Affiliate recruitment. We don’t work in Russian Federation and CIS. My fee is $400 per decryption. Contact details for builds and support [email protected]*

No Public Decryption Tool Available for the New Dharma variant

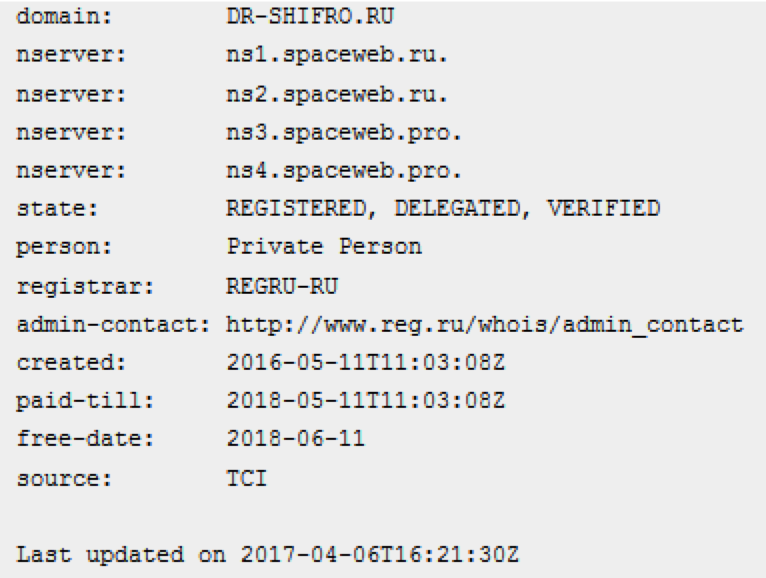
After researching several samples to ensure that the encryption algorithms did not contain any vulnerabilities, we found that in order to encrypt a victim's files, the ransomware implements the AES-256 algorithm and an AES key is encrypted with RSA-1024 and stored within the extra data chunk which is appended to each encrypted file.

For RSA encryption a public key embedded into the malware's binary is also used. In addition, the researched samples contained different RSA public keys that are not present in the list of previously released master keys. As a result, files encrypted with a new version of the ransomware cannot be decrypted with *any* of the publicly available decryption tools.

However, a Russian company named 'Dr. Shifro', claims to indeed be able to decrypt files encrypted by any new version of the Crisis/Dharma ransomware.

Dr. Shifro to the Rescue…

Opening business in 2016, coincidentally the same time that the first Crisis/Dharma ransomware campaigns began, 'Dr.Shifro' claims on its website to be "the only company specializing in data decryption after ransomware attacks". Other than Dharma, ransomware families covered by the service according to the website include Scarab, No_More_Ransom and Da Vinci.

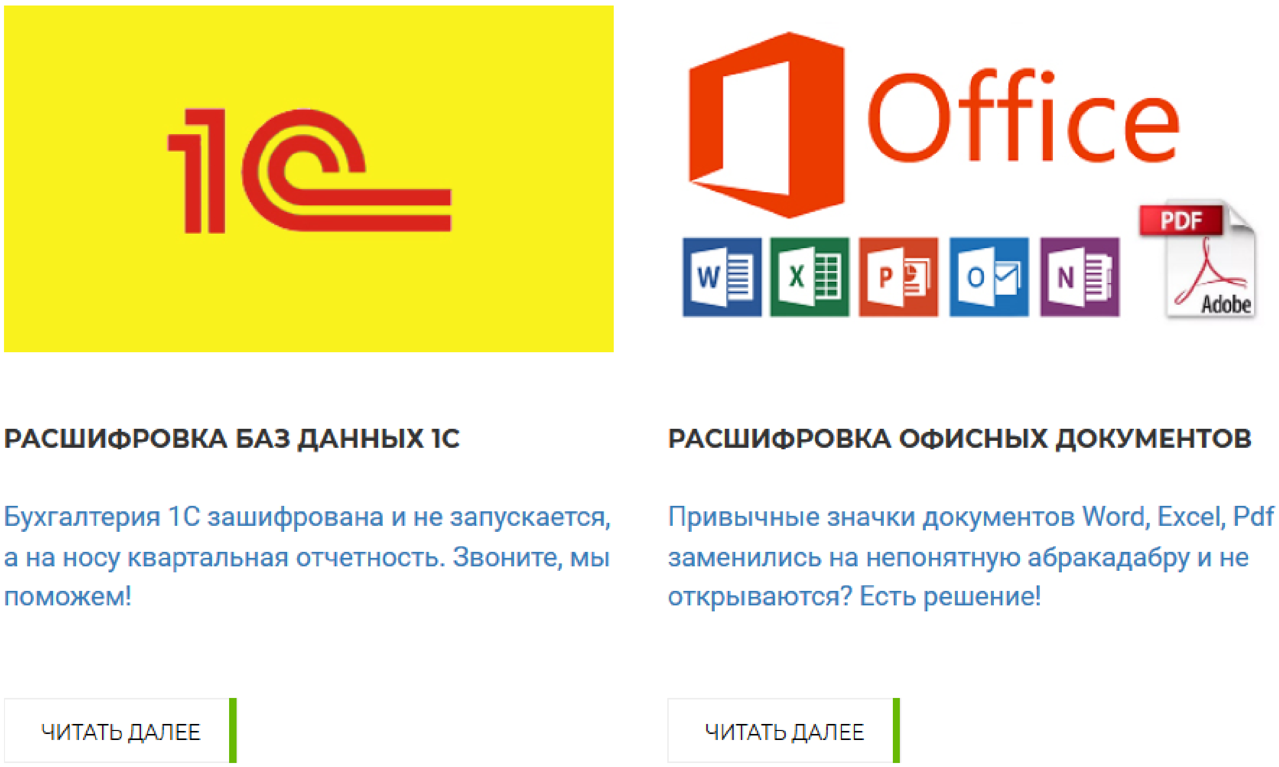


```
domain:        DR-SHIFRO.RU
nserver:       ns1.spaceweb.ru.
nserver:       ns2.spaceweb.ru.
nserver:       ns3.spaceweb.pro.
nserver:       ns4.spaceweb.pro.
state:         REGISTERED, DELEGATED, VERIFIED
person:        Private Person
registrar:     REGRU-RU
admin-contact: http://www.reg.ru/whois/admin_contact
created:       2016-05-11T11:03:08Z
paid-till:     2018-05-11T11:03:08Z
free-date:     2018-06-11
source:        TCI

Last updated on 2017-04-06T16:21:30Z
```

Figure 4: The *whois* data for the 'dr-shifro.ru' domain name.

According to the information published on the Dr. Shifro website, the company claims to help victims with the decryption of "1C" databases and Microsoft Office documents.



РАСШИФРОВКА БАЗ ДАННЫХ 1С

Бухгалтерия 1С зашифрована и не запускается, а на носу квартальная отчетность. Звоните, мы поможем!

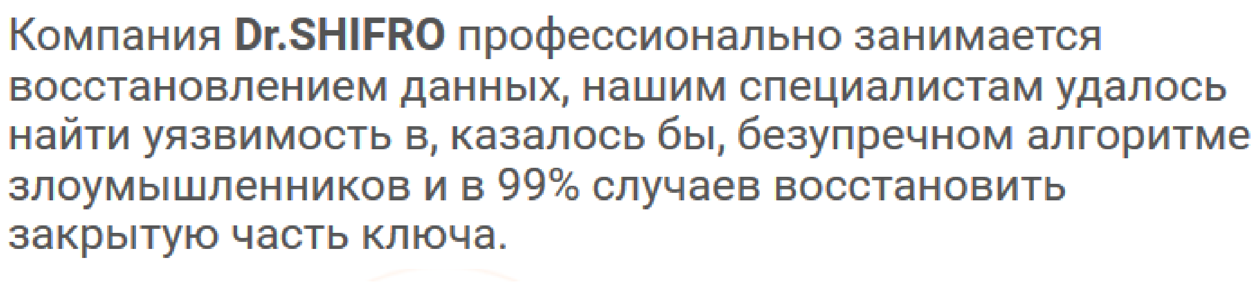
РАСШИФРОВКА ОФИСНЫХ ДОКУМЕНТОВ

Привычные значки документов Word, Excel, Pdf заменились на непонятную абракадабру и не открываются? Есть решение!

Figure 5: Dr. Shifro decryption services advertisements as seen on the Dr. Shifro website.

Translation: *Decryption of 1C databases. "1C:accounting" encrypted and doesn't run and quarterly reporting begins. Call us, we'll help! [Read more]*
Decryption of office documents. Regular icons of Word, Excel, Pdf documents have changed to something weird and don't open? Here is a solution! [Read more]

Another claim on the website says that in the vast majority of cases. Dr. Shifro exploits vulnerabilities in encryption algorithms of ransomware that allows them to restore RSA private keys.



Компания **Dr.SHIFRO** профессионально занимается восстановлением данных, нашим специалистам удалось найти уязвимость в, казалось бы, безупречном алгоритме злоумышленников и в 99% случаев восстановить закрытую часть ключа.

Figure 6: Dr. Shifro advertisement message.
Translation: *Dr. SHIFRO company engages in professional data recovery. Our experts have found a vulnerability in the algorithm of malware operators that appeared to be flawless,*

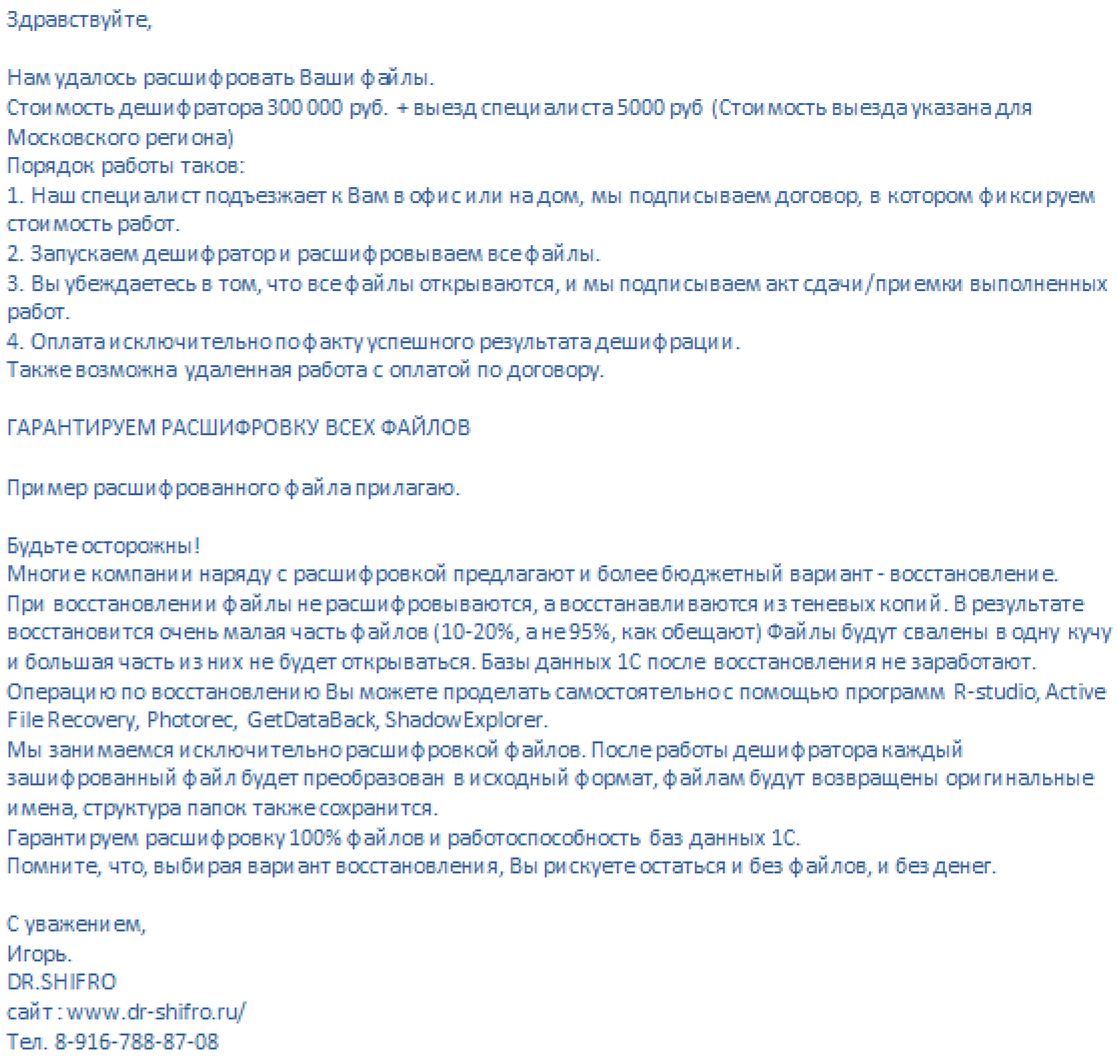
which allows us to restore a private key that has been used for encryption of users' files in 99% of cases.

However, as mentioned above, in case of Dharma ransomware an RSA public key is embedded into each sample and not generated at the victim's end. Therefore, the message above (Figure 5) could only mean that Dr. Shifro is able to break RSA-1024. Highly doubtful this is indeed the case, we began wondering – Could it be possible that Dr. Shifro is receiving its customers' recovered files from the only actor with access to the RSA keys – the ransomware operators?

That would mean that Dr. Shifro has been misleading the Dharma ransomware victims by posing as a legitimate company, when in reality, it merely functions as a broker between the attackers and their victims to maximize the operation's profits.

Our Investigation Begins

In order to understand Dr. Shifro's 'decryption process', we managed to get hold of one of their customer's correspondence with them. In this customer's case, they had been infected with a recent .gamma version of Dharma with an RSA key absent in the list of published master keys. After the customer had contacted Dr.Shifro and sent them some of their encrypted files via the email published on the company's website ([email protected]), a Dr. Shifro representative had responded instantly (within 2 hours) and returned the files decrypted.



Здравствуйте,

Нам удалось расшифровать Ваши файлы.
Стоимость дешифратора 300 000 руб. + выезд специалиста 5000 руб (Стоимость выезда указана для Московского региона)
Порядок работы таков:
1. Наш специалист подъезжает к Вам в офис или на дом, мы подписываем договор, в котором фиксируем стоимость работ.
2. Запускаем дешифратор и расшифровываем все файлы.
3. Вы убеждаетесь в том, что все файлы открываются, и мы подписываем акт сдачи/приемки выполненных работ.
4. Оплата исключительно по факту успешного результата дешифрации.
Также возможна удаленная работа с оплатой по договору.

ГАРАНТИРУЕМ РАСШИФРОВКУ ВСЕХ ФАЙЛОВ

Пример расшифрованного файла прилагаю.

Будьте осторожны!
Многие компании наряду с расшифровкой предлагают и более бюджетный вариант - восстановление.
При восстановлении файлы не расшифровываются, а восстанавливаются из теневых копий. В результате восстановится очень малая часть файлов (10-20%, а не 95%, как обещают) Файлы будут свалены в одну кучу и большая часть из них не будет открываться. Базы данных 1С после восстановления не заработают.
Операцию по восстановлению Вы можете проделать самостоятельно с помощью программ R-studio, Active File Recovery, Photorec, GetDataBack, ShadowExplorer.
Мы занимаемся исключительно расшифровкой файлов. После работы дешифратора каждый зашифрованный файл будет преобразован в исходный формат, файлам будут возвращены оригинальные имена, структура папок также сохранится.
Гарантируем расшифровку 100% файлов и работоспособность баз данных 1С.
Помните, что, выбирая вариант восстановления, Вы рискуете остаться и без файлов, и без денег.

С уважением,
Игорь.
DR.SHIFRO
сайт : www.dr-shifro.ru/
Тел. 8-916-788-87-08

Figure 7: Dr. Shifro’s response to a victim of the Dharma ransomware

Translation:
We managed to decrypt your files. Cost of the decryption tool is 300 000 rubles + visit by specialist 5000 rubles (the cost is for Moscow region).
Operating procedure is the following:
1. Our specialist visits you at home or at office. We sign the contract in which we fix the cost of services.
2. Run the decryption tool and decrypting all the files.
3. You unsure that all files opened. Then we sign statements of acceptance/delivery.
4. You pay only in case of successful decryption.
Also remote work is possible with payment under contract.
We guarantee the decryption of all files.
An example of the decrypted file is in the attachment.

Such a quick response time could only mean that either Dr. Shifro has RSA private keys for this infection case or he instantly interacts with the ransomware’s operator to receive them.

To know Dr. Shifro's process for sure, there was only one way to find out. We would need to carry out our own investigation. And as we had assumed the organization acts as merely a broker, we would need to control both sides of the attack chain – the ransomware operator and the ransomware victim.

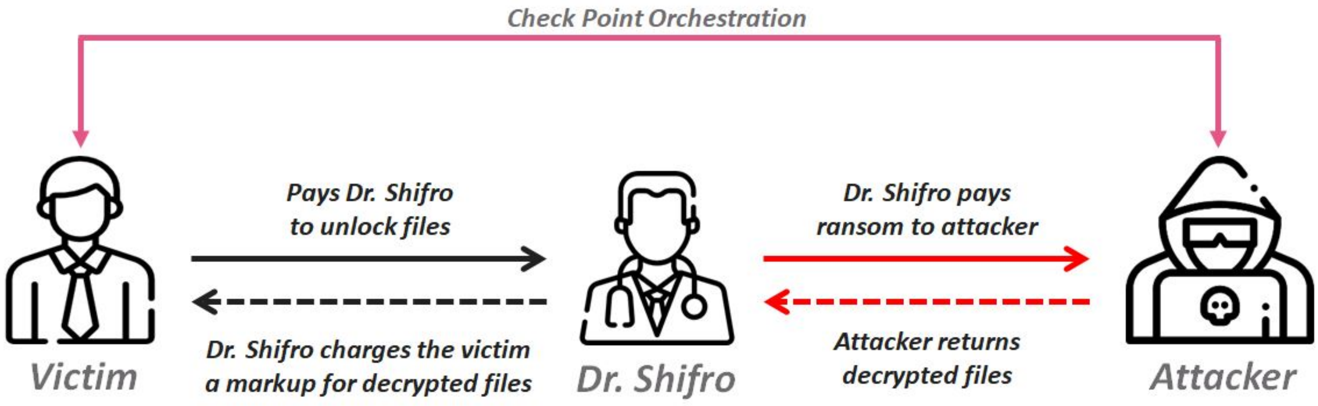

Check Point Orchestration
Pays Dr. Shifro to unlock files
Dr. Shifro charges the victim a markup for decrypted files
Dr. Shifro pays ransom to attacker
Attacker returns decrypted files
Victim
Dr. Shifro
Attacker

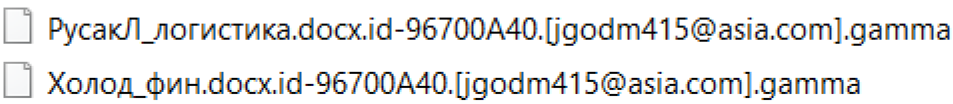
Figure 8: Check Point infiltration scheme

Setting Up the Investigation

Before setting our plan into action, and in order to correspond with Dr. Shifro as both the 'Ransomware Victim' and the 'Ransomware Operator', we would first need to register email addresses:

- [email protected] – Fake Ransomware Operator
- [email protected] – Fake malware operator (additional email)
- [email protected] – Fake Victim

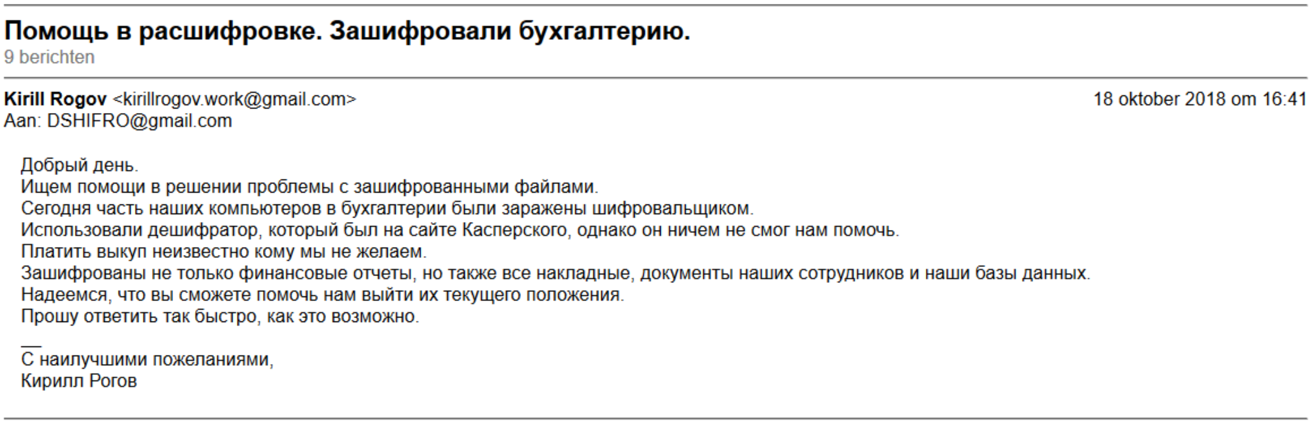
We then encrypted several files with a newly-created RSA-1024 public key, using the algorithm ripped from the ransomware. The names of the encrypted files also contained the email of the fake Ransomware Operator.



РусакЛ_логистика.docx.id-96700A40.[jgodm415@asia.com].gamma
Холод_фин.docx.id-96700A40.[jgodm415@asia.com].gamma

Figure 9: Files encrypted with the newly-created RSA key.

Following this, we then sent a message to Dr. Shifro using his website's email, ([email protected]) on behalf of the fake 'Ransomware victim'. Our email explained how we had recently become a ransomware victim and were looking for help with decrypting our files:



Помощь в расшифровке. Зашифровали бухгалтерию.
9 berichten

Kirill Rogov <kirillrogov.work@gmail.com> 18 oktober 2018 om 16:41
Aan: DSHIFRO@gmail.com

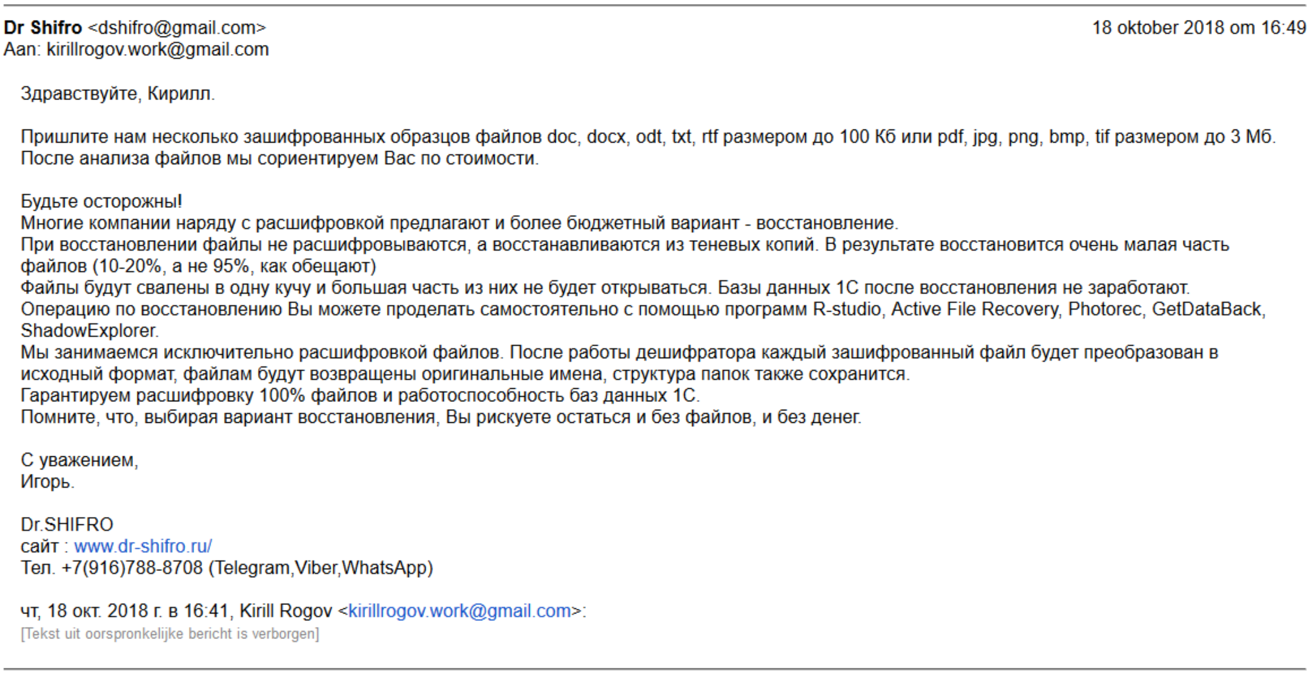
Добрый день.
Ищем помощи в решении проблемы с зашифрованными файлами.
Сегодня часть наших компьютеров в бухгалтерии были заражены шифровальщиком.
Использовали дешифратор, который был на сайте Касперского, однако он ничем не смог нам помочь.
Платить выкуп неизвестно кому мы не желаем.
Зашифрованы не только финансовые отчеты, но также все накладные, документы наших сотрудников и наши базы данных.
Надеемся, что вы сможете помочь нам выйти их текущего положения.
Прошу ответить так быстро, как это возможно.

__
С наилучшими пожеланиями,
Кирилл Рогов

Figure 10: Our initial message to Dr. Shifro on behalf of the fake ransomware victim.

Translation: *Looking for help with decryption of encrypted files. Today a part of our PCs in accounting department was infected with ransomware. We tried to use decryption tool from Kaspersky's website, but it didn't help us. We are not going to pay a ransom to unknown person… Please reply as soon as possible.*

After a few minutes we received a reply from Dr. Shifro in which we were asked to send several encrypted files as a sample in order to determine the level of difficulty to decrypt them and the subsequent price to do so. He also cautioned us against using the services of other companies in the meantime.



Dr Shifro <dshifro@gmail.com> 18 oktober 2018 om 16:49
Aan: kirillrogov.work@gmail.com

Здравствуйте, Кирилл.

Пришлите нам несколько зашифрованных образцов файлов doc, docx, odt, txt, rtf размером до 100 Кб или pdf, jpg, png, bmp, tif размером до 3 Мб.
После анализа файлов мы сориентируем Вас по стоимости.

Будьте осторожны!
Многие компании наряду с расшифровкой предлагают и более бюджетный вариант - восстановление.
При восстановлении файлы не расшифровываются, а восстанавливаются из теневых копий. В результате восстановится очень малая часть файлов (10-20%, а не 95%, как обещают)
Файлы будут свалены в одну кучу и большая часть из них не будет открываться. Базы данных 1С после восстановления не заработают.
Операцию по восстановлению Вы можете проделать самостоятельно с помощью программ R-studio, Active File Recovery, Photorec, GetDataBack, ShadowExplorer.
Мы занимаемся исключительно расшифровкой файлов. После работы дешифратора каждый зашифрованный файл будет преобразован в исходный формат, файлам будут возвращены оригинальные имена, структура папок также сохранится.
Гарантируем расшифровку 100% файлов и работоспособность баз данных 1С.
Помните, что, выбирая вариант восстановления, Вы рискуете остаться и без файлов, и без денег.

С уважением,
Игорь.

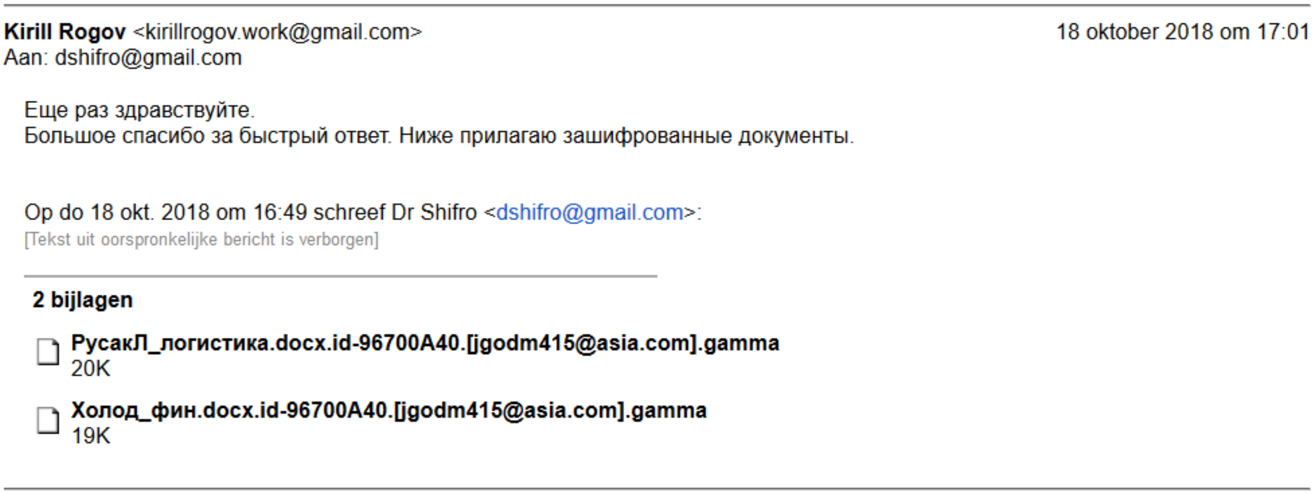
Dr.SHIFRO
сайт : www.dr-shifro.ru/
Тел. +7(916)788-8708 (Telegram,Viber,WhatsApp)

чт, 18 окт. 2018 г. в 16:41, Kirill Rogov <kirillrogov.work@gmail.com>:
[Tekst uit oorspronkelijke bericht is verborgen]

Figure 11: The Dr.Shifro's reply to the fake 'Ransomware Victim'.

Translation: *Send us several samples of encrypted files: doc, docx, odt, txt, rtf which size is less than 100Kb or pdf, jpg, png, bmp which size is less than 3Mb.*
After analyzing the files we will be able to estimate the cost of our service.

We then replied with the attached files we had ourselves previously encrypted:



Kirill Rogov <kirillrogov.work@gmail.com> 18 oktober 2018 om 17:01
Aan: dshifro@gmail.com

Еще раз здравствуйте.
Большое спасибо за быстрый ответ. Ниже прилагаю зашифрованные документы.

Op do 18 okt. 2018 om 16:49 schreef Dr Shifro <dshifro@gmail.com>:
[Tekst uit oorspronkelijke bericht is verborgen]

2 bijlagen

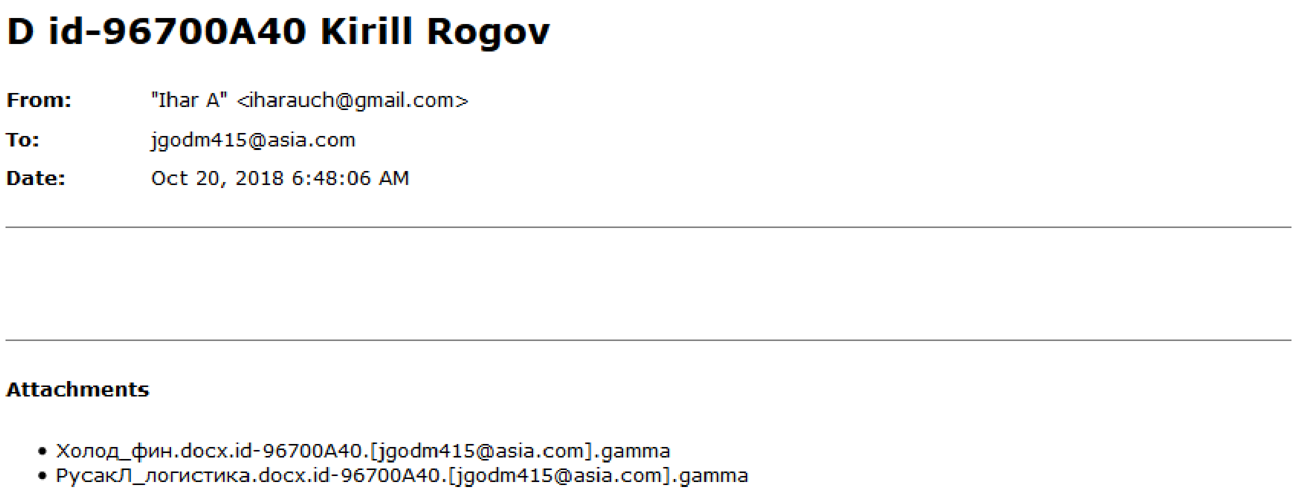
РусакЛ_логистика.docx.id-96700A40.[jgodm415@asia.com].gamma
20K

Холод_фин.docx.id-96700A40.[jgodm415@asia.com].gamma
19K

Figure 12: The message to “Dr.Shifro” with the encrypted files attached.

After this response Dr. Shifro went silent for two days. Of course, they were unable to decrypt files instantly because they did not have the RSA private key. In addition, the long delay could well have been due to them needing time to contact the various ransomware operators with which they have partnerships and try to obtain the relevant decryption key for this new customer.

On October 20, however, we received the following message into our fake ‘Ransomware Operator’ inbox. It was from email address “*[email protected]*”:



D id-96700A40 Kirill Rogov

From: "Ihar A" <iharauch@gmail.com>
To: jgodm415@asia.com
Date: Oct 20, 2018 6:48:06 AM

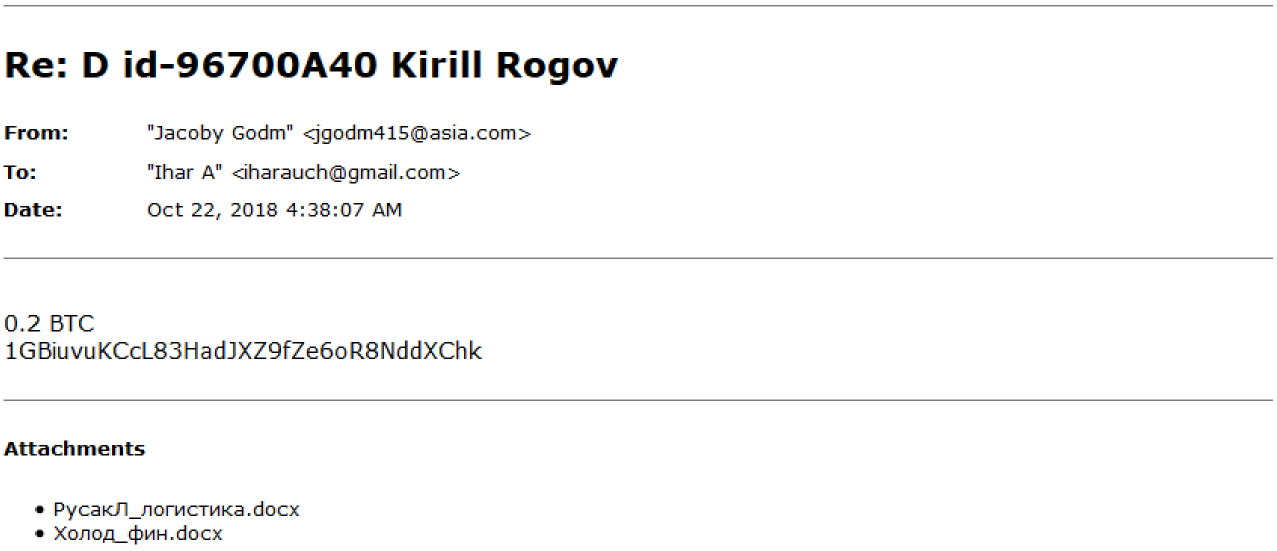
Attachments

- Холод_фин.docx.id-96700A40.[jgodm415@asia.com].gamma
- РусакЛ_логистика.docx.id-96700A40.[jgodm415@asia.com].gamma

Figure 13: The message to fake ransomware operator from a person behind “Dr.Shifro”.

We should emphasize here that the email address of the fake ransomware operator, “[email protected]” was known only to us and Dr.Shifro. Therefore the address “[email protected]” definitely belonged to the individual behind Dr.Shifro.

In response to Dr. Shifro’s email, and posing as the fake ‘Ransomware Operator’, we replied with the decrypted version of the files that we had received attached and the ransom amount and bitcoin address to where payment should be made.



Re: D id-96700A40 Kirill Rogov

From:	"Jacoby Godm" <jgodm415@asia.com>
To:	"Ihar A" <iharauch@gmail.com>
Date:	Oct 22, 2018 4:38:07 AM

0.2 BTC
1GBiuvuKCcL83HadJXZ9fZe6oR8NddXChk

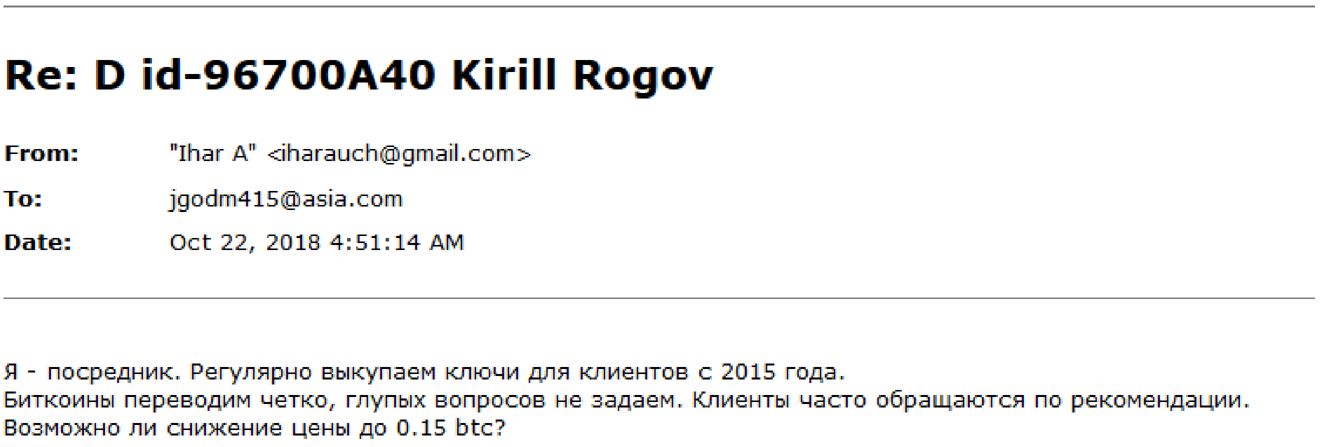
Attachments

- РусакЛ_логистика.docx
- Холод_фин.docx

Figure 14: Our reply on behalf of ransomware operator.

Following this initial correspondence we then received a reply from Dr. Shifro, again from email [email protected], in which they revealed how their business model works.

He explained that he is a mediator and regularly redeems keys for clients, sending bitcoin without any questions. He then asked for a discount on the 0.2 BTC we had requested to 0.15 BTC for the key. At this point we stopped communication.



Re: D id-96700A40 Kirill Rogov

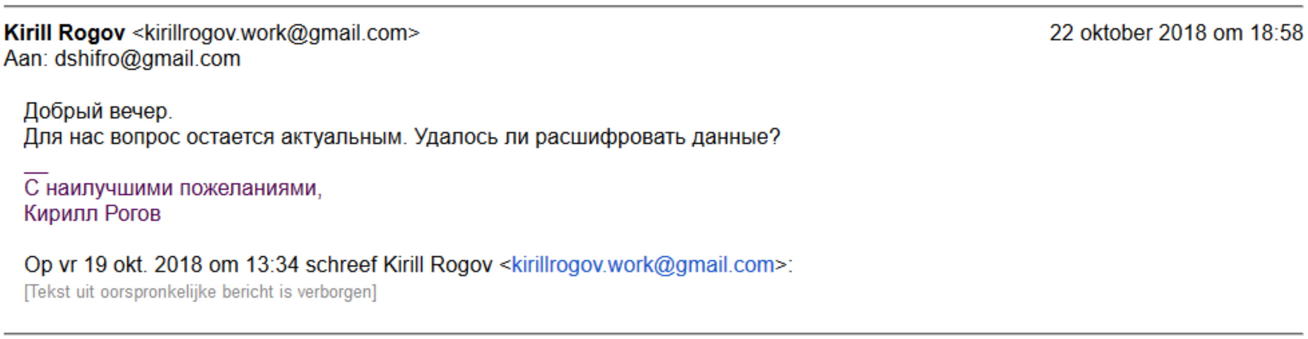
From: "Ihar A" <iharauch@gmail.com>
To: jgodm415@asia.com
Date: Oct 22, 2018 4:51:14 AM

Я - посредник. Регулярно выкупаем ключи для клиентов с 2015 года.
Биткоины переводим четко, глупых вопросов не задаем. Клиенты часто обращаются по рекомендации.
Возможно ли снижение цены до 0.15 btc?

Figure 15: Response of the person behind Dr. Shifro to the fake ‘Ransomware Operator’.

Translation: *I’m an intermediary. We redeem keys for clients since 2015 on a regular basis. Send bitcoins tight, don’t ask dumb questions.*
Clients frequently addressed under recommendation. Could you give a discount to 0.15 btc?

To understand the exact profit margin added by Dr.Shifro to the initial ransom price, this time posing as the fake victim we then contacted them again to ask for a status update.



Kirill Rogov <kirillrogov.work@gmail.com> 22 oktober 2018 om 18:58
Aan: dshifro@gmail.com

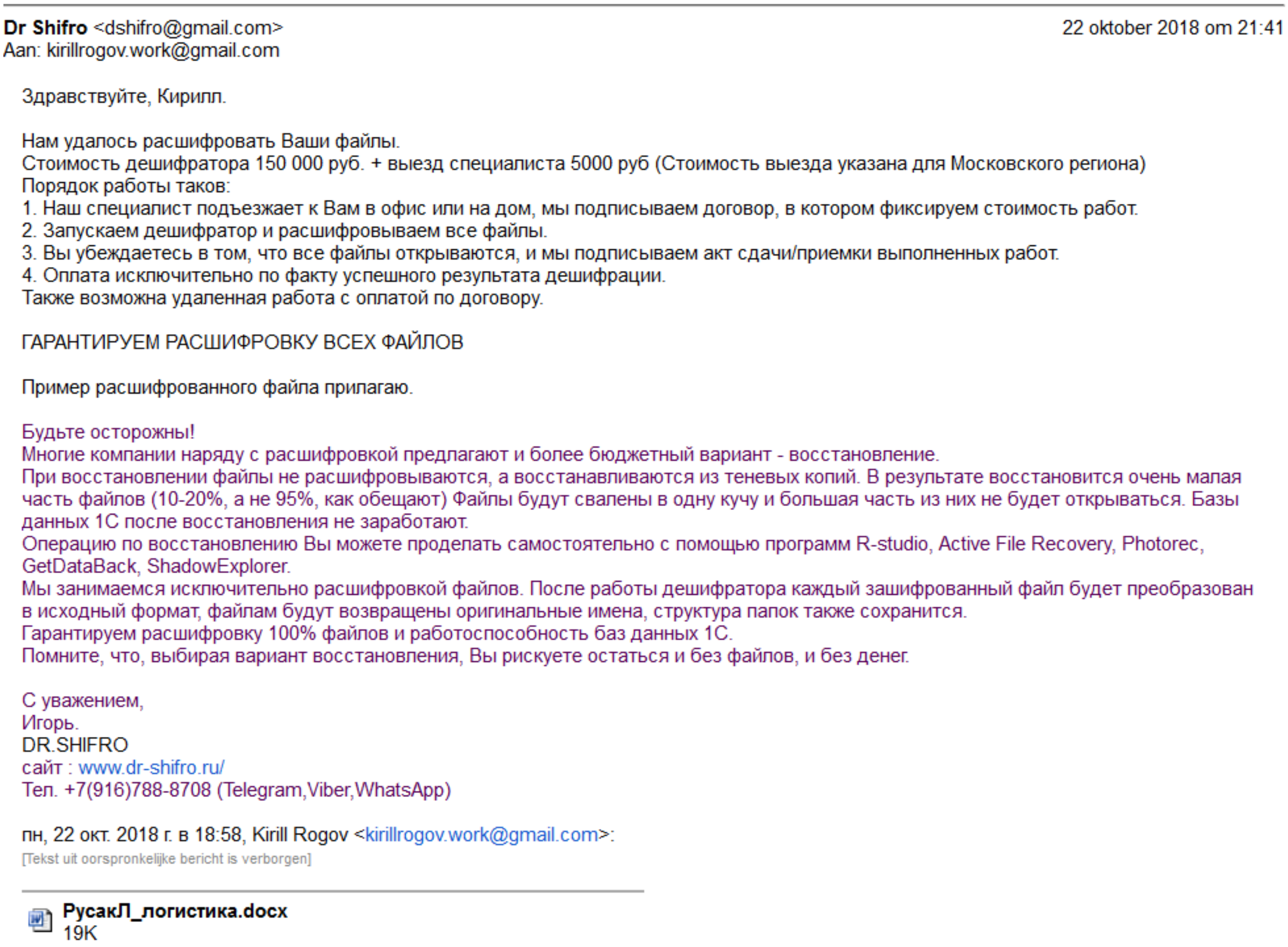
Добрый вечер.
Для нас вопрос остается актуальным. Удалось ли расшифровать данные?

__
С наилучшими пожеланиями,
Кирилл Рогов

Op vr 19 okt. 2018 om 13:34 schreef Kirill Rogov <kirillrogov.work@gmail.com>:
[Tekst uit oorspronkelijke bericht is verborgen]

Figure 16: The fake ‘Ransomware Victim’s request for a status update.

We finally received a response from Dr. Shifro in which they informed us, the victim, that the files were successfully decrypted (a sample was attached) and that the price was 150,000 Russian Rubles (approx. $2300).



Dr Shifro <dshifro@gmail.com> 22 oktober 2018 om 21:41
Aan: kirillrogov.work@gmail.com

Здравствуйте, Кирилл.

Нам удалось расшифровать Ваши файлы.
Стоимость дешифратора 150 000 руб. + выезд специалиста 5000 руб (Стоимость выезда указана для Московского региона)
Порядок работы таков:
1. Наш специалист подъезжает к Вам в офис или на дом, мы подписываем договор, в котором фиксируем стоимость работ.
2. Запускаем дешифратор и расшифровываем все файлы.
3. Вы убеждаетесь в том, что все файлы открываются, и мы подписываем акт сдачи/приемки выполненных работ.
4. Оплата исключительно по факту успешного результата дешифрации.
Также возможна удаленная работа с оплатой по договору.

ГАРАНТИРУЕМ РАСШИФРОВКУ ВСЕХ ФАЙЛОВ

Пример расшифрованного файла прилагаю.

Будьте осторожны!
Многие компании наряду с расшифровкой предлагают и более бюджетный вариант - восстановление.
При восстановлении файлы не расшифровываются, а восстанавливаются из теневых копий. В результате восстановится очень малая часть файлов (10-20%, а не 95%, как обещают) Файлы будут свалены в одну кучу и большая часть из них не будет открываться. Базы данных 1С после восстановления не заработают.
Операцию по восстановлению Вы можете проделать самостоятельно с помощью программ R-studio, Active File Recovery, Photorec, GetDataBack, ShadowExplorer.
Мы занимаемся исключительно расшифровкой файлов. После работы дешифратора каждый зашифрованный файл будет преобразован в исходный формат, файлам будут возвращены оригинальные имена, структура папок также сохранится.
Гарантируем расшифровку 100% файлов и работоспособность баз данных 1С.
Помните, что, выбирая вариант восстановления, Вы рискуете остаться и без файлов, и без денег.

С уважением,
Игорь.
DR.SHIFRO
сайт : www.dr-shifro.ru/
Тел. +7(916)788-8708 (Telegram,Viber,WhatsApp)

пн, 22 окт. 2018 г. в 18:58, Kirill Rogov <kirillrogov.work@gmail.com>:
[Tekst uit oorspronkelijke bericht is verborgen]

РусакЛ_логистика.docx
19K

Figure 17: Response from “Dr.Shifro” to the victim.

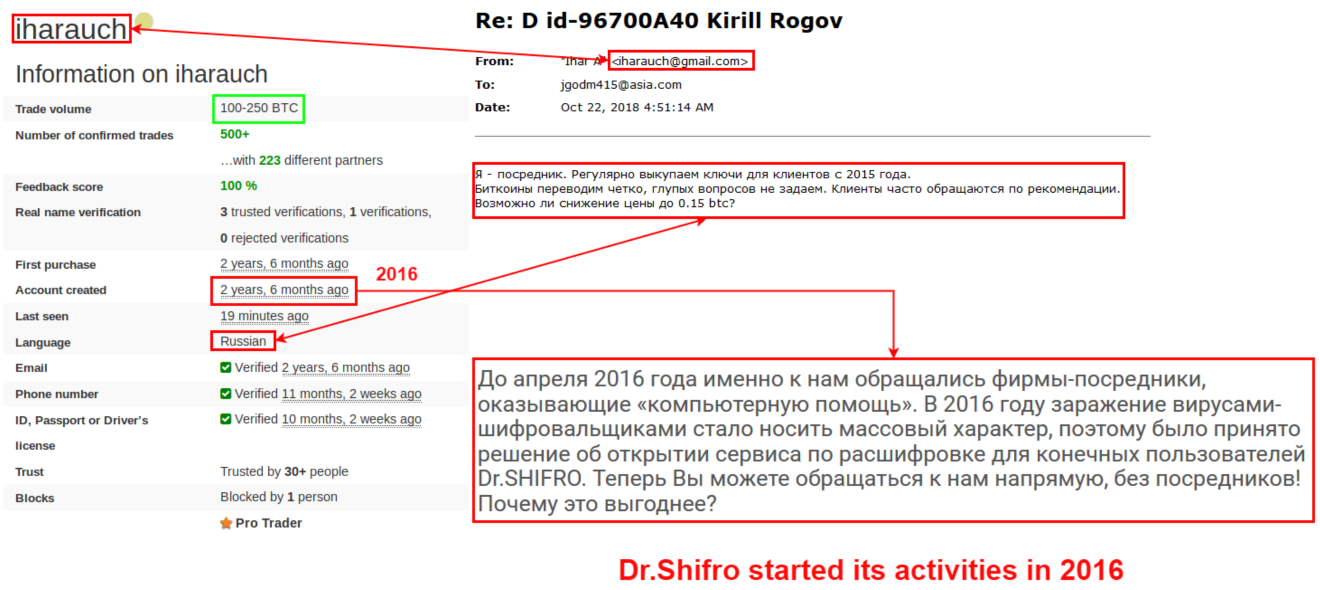
Translation: *We managed to decrypt your files. Cost of the decryption tool is 150 000 rubles + visit by specialist 5000 rubles (the cost is for Moscow region)…*

Dr. Shifro requested to pay us, the ‘ransomware distributors’, 0.15 btc, the equivalent of approximately $950 at the time, and charged the ransomware victim 150,000 rubles, worth approximately $2300. This means the company would earn around $1350 from a single victim.

Threat Actor Doxing

[email protected]

As mentioned above, our fake ‘Ransomware Operator’ received messages from the email address, *[email protected]*. Crossing multiple sources, we managed to determine that *iharauch* is a unique user’s avatar. Using this identifier a profile at *localbitcoins.com* platform was easily found:



iharauch

Information on iharauch

Trade volume	100-250 BTC
Number of confirmed trades	500+
	…with 223 different partners
Feedback score	100 %
Real name verification	3 trusted verifications, 1 verifications,
	0 rejected verifications
First purchase	2 years, 6 months ago
Account created	2 years, 6 months ago
Last seen	19 minutes ago
Language	Russian
Email	☑ Verified 2 years, 6 months ago
Phone number	☑ Verified 11 months, 2 weeks ago
ID, Passport or Driver's license	☑ Verified 10 months, 2 weeks ago
Trust	Trusted by 30+ people
Blocks	Blocked by 1 person
	★ Pro Trader

2016

Re: D id-96700A40 Kirill Rogov

From: "Ihar A" <iharauch@gmail.com>
To: jgodm415@asia.com
Date: Oct 22, 2018 4:51:14 AM

Я - посредник. Регулярно выкупаем ключи для клиентов с 2015 года.
Биткоины переводим четко, глупых вопросов не задаем. Клиенты часто обращаются по рекомендации.
Возможно ли снижение цены до 0.15 btc?

До апреля 2016 года именно к нам обращались фирмы-посредники, оказывающие «компьютерную помощь». В 2016 году заражение вирусами-шифровальщиками стало носить массовый характер, поэтому было принято решение об открытии сервиса по расшифровке для конечных пользователей Dr.SHIFRO. Теперь Вы можете обращаться к нам напрямую, без посредников! Почему это выгоднее?

Dr.Shifro started its activities in 2016

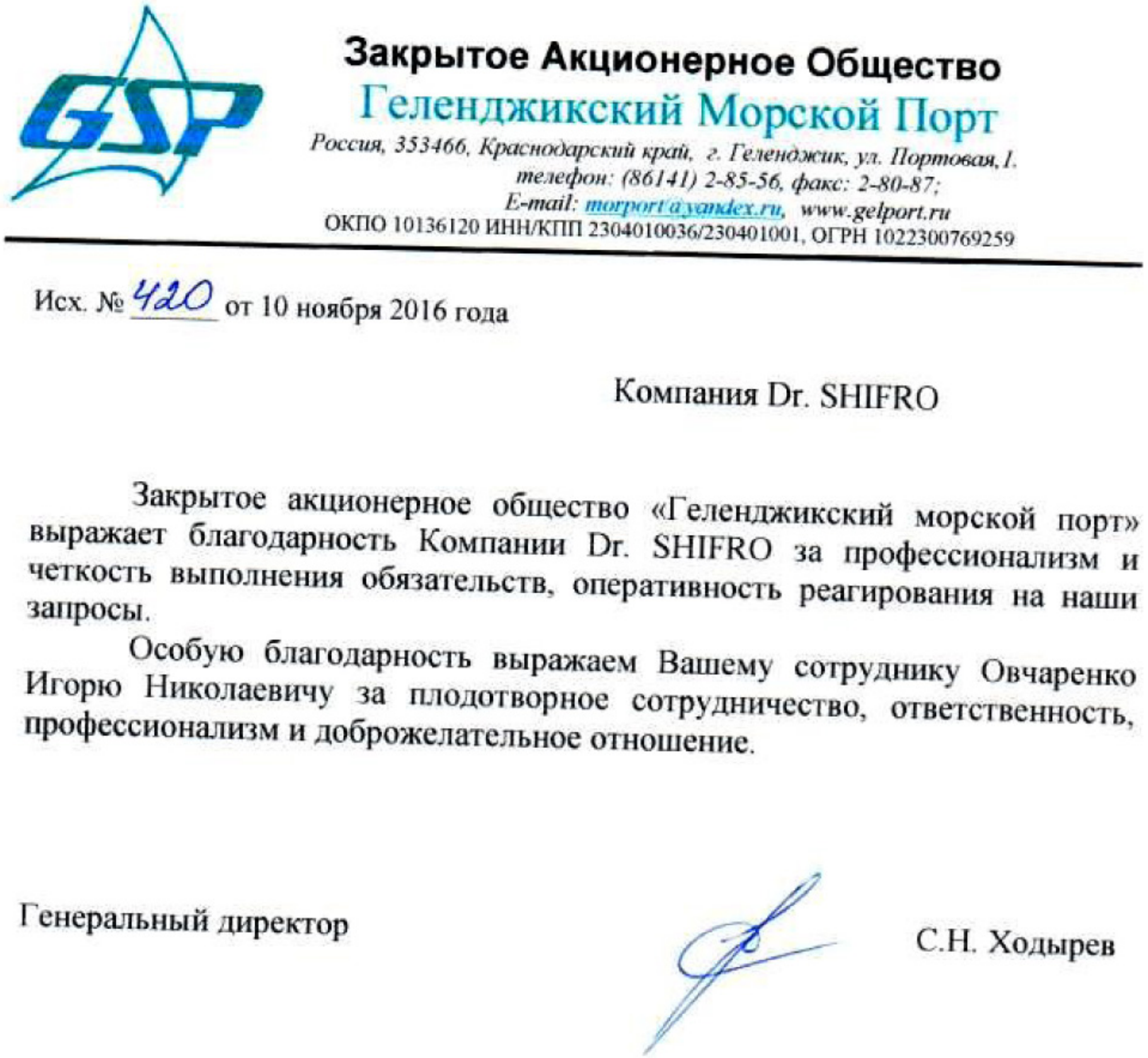
Figure 18: *iharauch* profile at *localbitcoins.com.*

The trading volume on this account, which signifies the amount of BTC purchased by our actor, enables us to estimate the amount of decryption keys Dr. Shifro bought since 2016, and the profit he gained as an intermediary between victims and ransomware operators.

The average BTC value for the examined time was $3000, and the trading volume of Dr. Shifro's account is at least 100 BTC – which means that the actor spend at least $300,000 on key purchase. Our investigation revealed that Dr. Shifro pays approximately $950 for each key – which means that the actor made at least 315 deals. Taking into account that Dr. Shifro could have earned $1350 in net profit from the deal we allegedly initiated, we can estimate that the business yielded at least $425,000. The profits could grow even higher if the same decryption keys have been used several times and Dr. Shifro could have sold a single key move than once.

Ovcharenko Igor Nikolaevich

Noting the various several thank-you letters published at the *dr-shifro.ru* web-site, we decided to take a closer look to see if we could garner any further information about Dr. Shifro. One such letter actually contains the supposed name of the person behind the Dr.Shifro Company – Mr. Igor Ovcharenko.



Закрытое Акционерное Общество

Геленджикский Морской Порт

Россия, 353466, Краснодарский край, г. Геленджик, ул. Портовая, 1.
телефон: (86141) 2-85-56, факс: 2-80-87;
E-mail: morport@yandex.ru, www.gelport.ru
ОКПО 10136120 ИНН/КПП 2304010036/230401001, ОГРН 1022300769259

Исх. № 420 от 10 ноября 2016 года

Компания Dr. SHIFRO

Закрытое акционерное общество «Геленджикский морской порт» выражает благодарность Компании Dr. SHIFRO за профессионализм и четкость выполнения обязательств, оперативность реагирования на наши запросы.

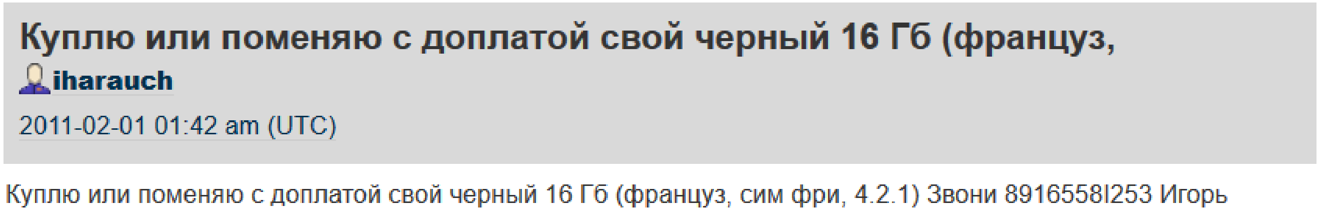
Особую благодарность выражаем Вашему сотруднику Овчаренко Игорю Николаевичу за плодотворное сотрудничество, ответственность, профессионализм и доброжелательное отношение.

Генеральный директор С.Н. Ходырев

Figure 19: Thank-you letter published at dr-shifro.ru.

Translation: *“Gelendzhik seaport” Closed Joint Stock Company thanked Dr. SHIFRO Company for professionalism, commitment and rapid response to our requests.*
We are particularly grateful to your employee Ovcharenko Igor Nikolaevich for fruitful cooperation, responsibility, professionalism and goodwill.

Using the “iharauch” identifier, an acknowledgment of a relation between the name and the “iharauch” avatar could be found:



Куплю или поменяю с доплатой свой черный 16 Гб (француз,

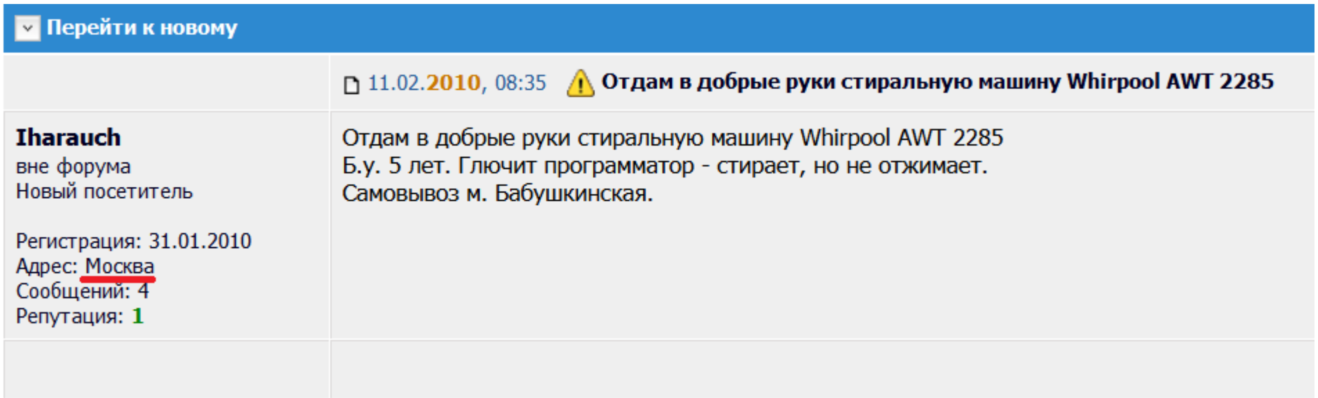
iharauch

2011-02-01 01:42 am (UTC)

Куплю или поменяю с доплатой свой черный 16 Гб (француз, сим фри, 4.2.1) Звони 8916558l253 Игорь

Figure 20: The connection between the avatar and the name "Igor".

Translation: *[I] would like to buy or exchange with a surcharge a 16 GB [iPhone] (French, sim-free, 4.2.1). Call 89165581253 Igor.*



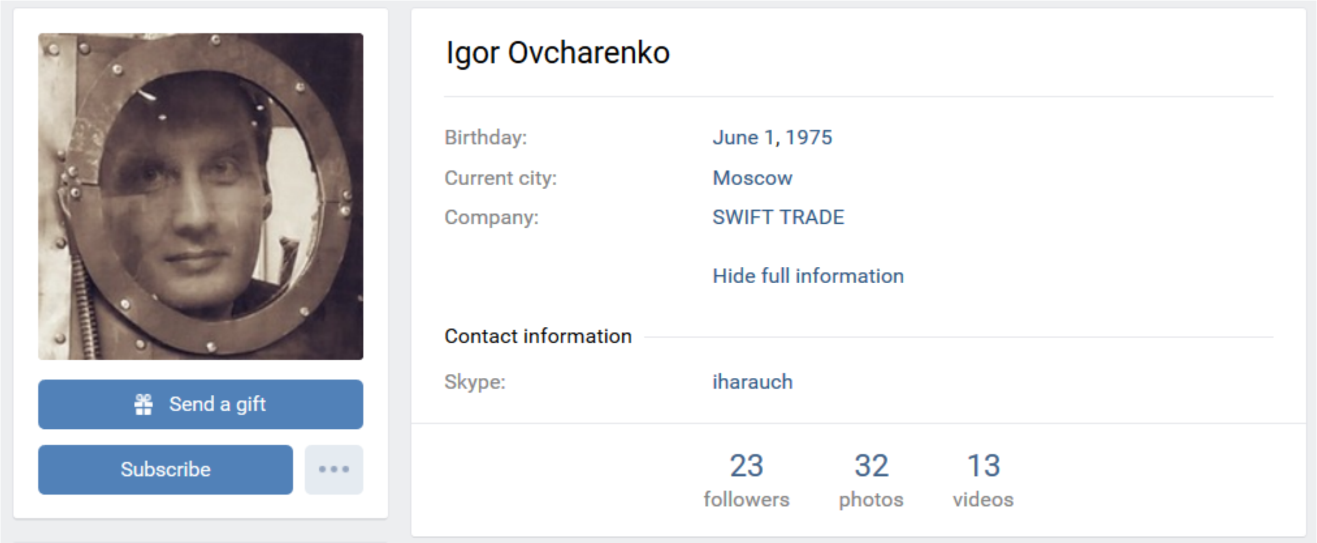
11.02.2010, 08:35 ⚠ **Отдам в добрые руки стиральную машину Whirpool AWT 2285**

Iharauch
вне форума
Новый посетитель

Регистрация: 31.01.2010
Адрес: Москва
Сообщений: 4
Репутация: 1

Отдам в добрые руки стиральную машину Whirpool AWT 2285
Б.у. 5 лет. Глючит программатор - стирает, но не отжимает.
Самовывоз м. Бабушкинская.

Figure 21: The location of the person is Moscow.



Igor Ovcharenko

Birthday: June 1, 1975
Current city: Moscow
Company: SWIFT TRADE

Contact information

Skype: iharauch

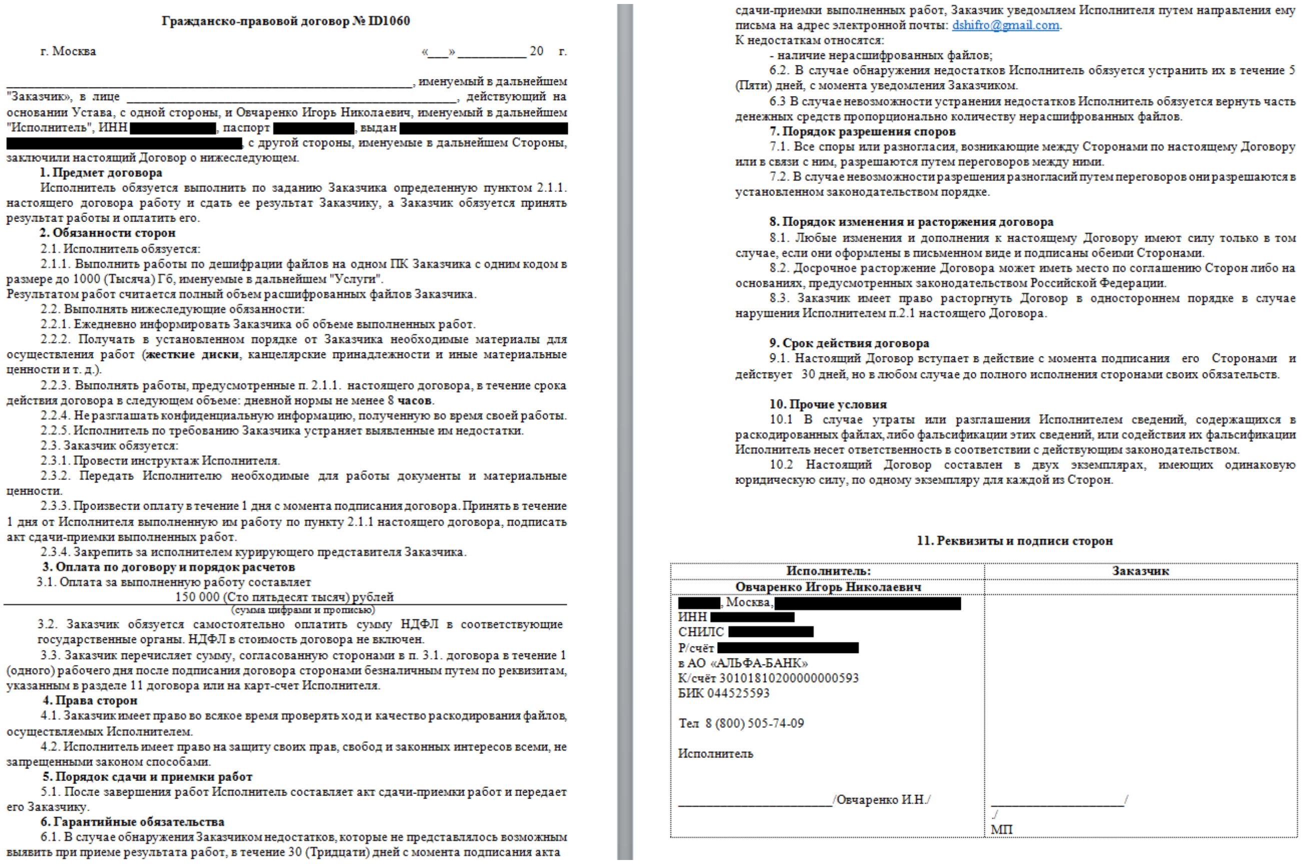
23 followers
32 photos
13 videos

Figure 22: "iharauch" profile *https://vk.com/id3556491*

Despite the fact that the VK.com social network profile of "iharauch" has not been updated since 2014, we were able to find other active profiles connect to the VK.com profile.

In order to obtain information about the legal status of the Dr.Shifro organization, we asked them, using our fake victim address, to send us a template of the contract which is usually signed before Dr. Shifro starts work on decrypting files. The response we received contained a template of a *civil contract* and a handful of personal registration documents of the person behind Dr.Shifro, including scans of his passport, registration of residence, insurance certificate and Internal Revenue Service certificate.

The civil contract contains personal data of a certain ‘Ovcharenko Igor Nikolaevich’ including passport details, taxpayer identification number and even personal bank credentials. The contract suggests the commitment to decrypt up to 1000GB of data using “one code” by the service contractor. In turn, the customer also commits to make payment of 150,000 Russian Rubles.



Гражданско-правовой договор № ID1060

г. Москва «___» __________ 20 г.

____, именуемый в дальнейшем "Заказчик», в лице ____, действующий на основании Устава, с одной стороны, и Овчаренко Игорь Николаевич, именуемый в дальнейшем "Исполнитель", ИНН [redacted], паспорт [redacted], выдан [redacted], с другой стороны, именуемые в дальнейшем Стороны, заключили настоящий Договор о нижеследующем.

1. Предмет договора

Исполнитель обязуется выполнить по заданию Заказчика определенную пунктом 2.1.1. настоящего договора работу и сдать ее результат Заказчику, а Заказчик обязуется принять результат работы и оплатить его.

2. Обязанности сторон

2.1. Исполнитель обязуется:

2.1.1. Выполнить работы по дешифрации файлов на одном ПК Заказчика с одним кодом в размере до 1000 (Тысяча) Гб, именуемые в дальнейшем "Услуги".

Результатом работ считается полный объем расшифрованных файлов Заказчика.

2.2. Выполнять нижеследующие обязанности:

2.2.1. Ежедневно информировать Заказчика об объеме выполненных работ.

2.2.2. Получать в установленном порядке от Заказчика необходимые материалы для осуществления работ (**жесткие диски**, канцелярские принадлежности и иные материальные ценности и т. д.).

2.2.3. Выполнять работы, предусмотренные п. 2.1.1. настоящего договора, в течение срока действия договора в следующем объеме: дневной нормы не менее 8 **часов**.

2.2.4. Не разглашать конфиденциальную информацию, полученную во время своей работы.

2.2.5. Исполнитель по требованию Заказчика устраняет выявленные им недостатки.

2.3. Заказчик обязуется:

2.3.1. Провести инструктаж Исполнителя.

2.3.2. Передать Исполнителю необходимые для работы документы и материальные ценности.

2.3.3. Произвести оплату в течение 1 дня с момента подписания договора. Принять в течение 1 дня от Исполнителя выполненную им работу по пункту 2.1.1 настоящего договора, подписать акт сдачи-приемки выполненных работ.

2.3.4. Закрепить за исполнителем курирующего представителя Заказчика.

3. Оплата по договору и порядок расчетов

3.1. Оплата за выполненную работу составляет

150 000 (Сто пятьдесят тысяч) рублей

(сумма цифрами и прописью)

3.2. Заказчик обязуется самостоятельно оплатить сумму НДФЛ в соответствующие государственные органы. НДФЛ в стоимость договора не включен.

3.3. Заказчик перечисляет сумму, согласованную сторонами в п. 3.1. договора в течение 1 (одного) рабочего дня после подписания договора сторонами безналичным путем по реквизитам, указанным в разделе 11 договора или на карт-счет Исполнителя.

4. Права сторон

4.1. Заказчик имеет право во всякое время проверять ход и качество раскодирования файлов, осуществляемых Исполнителем.

4.2. Исполнитель имеет право на защиту своих прав, свобод и законных интересов всеми, не запрещенными законом способами.

5. Порядок сдачи и приемки работ

5.1. После завершения работ Исполнитель составляет акт сдачи-приемки работ и передает его Заказчику.

6. Гарантийные обязательства

6.1. В случае обнаружения Заказчиком недостатков, которые не представлялось возможным выявить при приеме результата работ, в течение 30 (Тридцати) дней с момента подписания акта сдачи-приемки выполненных работ, Заказчик уведомляем Исполнителя путем направления ему письма на адрес электронной почты: dshifro@gmail.com.

К недостаткам относятся:

- наличие нерасшифрованных файлов;

6.2. В случае обнаружения недостатков Исполнитель обязуется устранить их в течение 5 (Пяти) дней, с момента уведомления Заказчиком.

6.3 В случае невозможности устранения недостатков Исполнитель обязуется вернуть часть денежных средств пропорционально количеству нерасшифрованных файлов.

7. Порядок разрешения споров

7.1. Все споры или разногласия, возникающие между Сторонами по настоящему Договору или в связи с ним, разрешаются путем переговоров между ними.

7.2. В случае невозможности разрешения разногласий путем переговоров они разрешаются в установленном законодательством порядке.

8. Порядок изменения и расторжения договора

8.1. Любые изменения и дополнения к настоящему Договору имеют силу только в том случае, если они оформлены в письменном виде и подписаны обеими Сторонами.

8.2. Досрочное расторжение Договора может иметь место по соглашению Сторон либо на основаниях, предусмотренных законодательством Российской Федерации.

8.3. Заказчик имеет право расторгнуть Договор в одностороннем порядке в случае нарушения Исполнителем п.2.1 настоящего Договора.

9. Срок действия договора

9.1. Настоящий Договор вступает в действие с момента подписания его Сторонами и действует 30 дней, но в любом случае до полного исполнения сторонами своих обязательств.

10. Прочие условия

10.1 В случае утраты или разглашения Исполнителем сведений, содержащихся в раскодированных файлах, либо фальсификации этих сведений, или содействия их фальсификации Исполнитель несет ответственность в соответствии с действующим законодательством.

10.2 Настоящий Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

11. Реквизиты и подписи сторон

Исполнитель:	Заказчик
Овчаренко Игорь Николаевич	
[redacted], Москва, [redacted] ИНН [redacted] СНИЛС [redacted] Р/счёт [redacted] в АО «АЛЬФА-БАНК» К/счёт 30101810200000000593 БИК 044525593 Тел 8 (800) 505-74-09 Исполнитель ______________________/Овчаренко И.Н./	____________________/ ./ МП

Figure 23: Dr.Shifro’s civil contract template.

Conclusion

Mr. Igor Ovcharenko runs a simple, organized and profitable business. As Dr. Shifro, he reaches out to customers in need of his help, victims hit by the ransomware families including Dharma, Scarab, No_More_Ransom and Da Vinci, for which no key is publicly available. He doesn’t operate under the radar though. Instead he maintains contact with his clients and partners throughout the process and binds his service with a civil contract. Furthermore, he even provides his personal credentials as part of the deal closure. This all enables Dr. Shifro to act as a legitimate business, though in reality Dr. Shifro’s services rely on its malice collaborators, ransomware distributors themselves.

Our case study, in which we formed direct contact with Dr. Shifro as both a ransomware distributor and victim, taught us that the company earns, on average, $1350 per customer, and over $200,000 per year. It is an efficient and easy-to-run business model that can significantly increase the profits generated by ransomware campaigns. Therefore, we may expect to see other threat actors running similar operations. Considering the recent decreasing popularity of ransomware in favor of cryptomining malware, the new and rising industry could enlarge the profits from ransomware attack campaigns and put this malware type back at the top of the charts.

GO UP
BACK TO ALL POSTS