

В чат група „tad cyber team“ е установена публикация, в която на 05.03.2019г. Иван Тодоров пише: „ Ще свалям правителството хаха“

The screenshot shows a Telegram chat window with a title bar containing icons for back, forward, search, and share, along with the text '3536 / 7036'. The chat content includes two messages from user '279562092 Ivan Todorov':

- The first message is in a blue bubble and reads: "_____ също е част от екипа, въпреки и външен. С него подписвам граждански договор." It is timestamped "5.3.2019 г. 13:03(UTC+0)".
- The second message is also in a blue bubble and reads: "Ще свалям правителството хаха". It is timestamped "5.3.2019 г. 13:04(UTC+0)".

Below each message, there is a 'Source:' field with technical details such as file paths and sizes.

На 21.06.2019г в същата група, Бойков публикува: „Ударихме на ... от машината и откраднахме всички документи“

The screenshot shows a Telegram chat window with three messages from user '571921516 John Doe':

- The first message is in a green bubble and reads: "Ударихме на _____ от _____ машината." It is timestamped "21.6.2019 г. 08:03(UTC+0)".
- The second message is in a green bubble and reads: "И откраднахме всички документи". It is timestamped "21.6.2019 г. 08:03(UTC+0)".
- The third message is in a green bubble and reads: "@chapoblan". It is timestamped "21.6.2019 г. 08:03(UTC+0)".

Each message has a 'Source:' field with technical details.

<p>571921516 John Doe @charoblan Status: Sent 21.6.2019 г. 08:03(UTC+0)</p>	
<p>zip/apps/org.telegram.messenger/Cache4.db : 0x1B588AE (Table: messages, zip/apps/org.telegram.messenger/Cache4.db-wal : 0xCCB8D (Table: users,</p>	High
<p>571921516 John Doe Със всички ИСА. Status: Sent 21.6.2019 г. 08:03(UTC+0)</p>	
<p>ip/apps/org.telegram.messenger/Cache4.db : 0x1B67FD7 (Table: messages, ip/apps/org.telegram.messenger/Cache4.db-wal : 0xCCB8D (Table: users,</p>	High
<p>279562092 Ivan Todorov ХАХХА 21.6.2019 г. 08:04(UTC+0)</p>	

Като около минута по-късно, служителите получават инструкция от Иван Тодоров да свалят всички пароли и да направят копие (*mirror image*) на информацията

<p>279562092 Ivan Todorov <u>свалете му всичко, пароли мароли</u> 21.6.2019 г. 08:05(UTC+0)</p>	<p>ip/apps/org.telegram.messenger/Cache4.db : 0x1B67CE4 (Table: messages, ip/apps/org.telegram.messenger/Cache4.db-wal : 0xCC2C9 (Table: users,</p>
<p>667684434 З [REDACTED] D 21.6.2019 г. 08:05(UTC+0)</p>	<p>zip/apps/org.telegram.messenger/Cache4.db : 0x1B67CA0 (Table: messages, zip/apps/org.telegram.messenger/Cache4.db-wal : 0xDE9CD (Table: users,</p>
<p>279562092 Ivan Todorov <u>направо mirror image</u> 21.6.2019 г. 08:05(UTC+0)</p>	<p>zip/apps/org.telegram.messenger/Cache4.db : 0x1B67CA9 (Table: messages, zip/apps/org.telegram.messenger/Cache4.db-wal : 0xCC2C9 (Table: users,</p>

И ДОПЪЛВА „ТО СЛЕД ВСЕКИ ОДИТ ИМА ПО ЕДИН УДАРЕН“

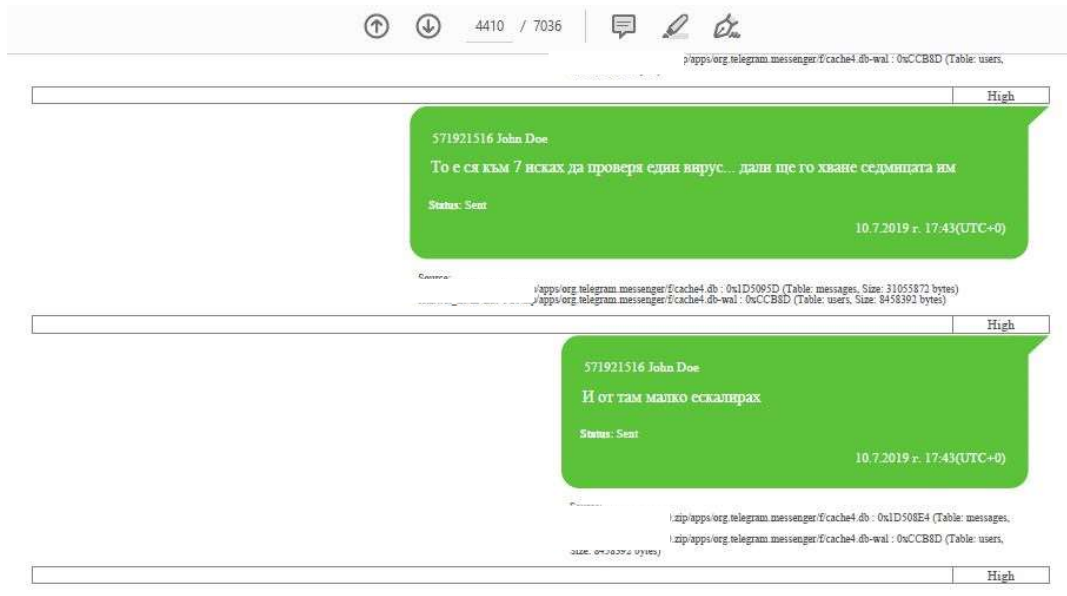
The screenshot shows a Telegram chat interface with three messages from a contact with ID 667684434. The messages are:

- Message 1: "да" (yes), timestamp: 21.6.2019 г. 08:05(UTC+0). Metadata: /zip/apps/org.telegram.messenger/f/cache4.db: 0x1B67C05 (Table: messages, Size: 8458392 bytes); /zip/apps/org.telegram.messenger/f/cache4.db-wal: 0xDE9CD (Table: users).
- Message 2: "ТО СЛЕД ВСЕКИ ОДИТ ИМА ПО ЕДИН УДАРЕН" (Underlined), timestamp: 21.6.2019 г. 08:06(UTC+0). Metadata: /zip/apps/org.telegram.messenger/f/cache4.db: 0x1B67B86 (Table: messages, Size: 8458392 bytes); /zip/apps/org.telegram.messenger/f/cache4.db-wal: 0xCC2C9 (Table: users).
- Message 3: "ХАХ" (HA HA), timestamp: 21.6.2019 г. 08:06(UTC+0). Metadata: /zip/apps/org.telegram.messenger/f/cache4.db: 0x1B67B41 (Table: messages, Size: 8458392 bytes); /zip/apps/org.telegram.messenger/f/cache4.db-wal: 0xCC2C9 (Table: users).

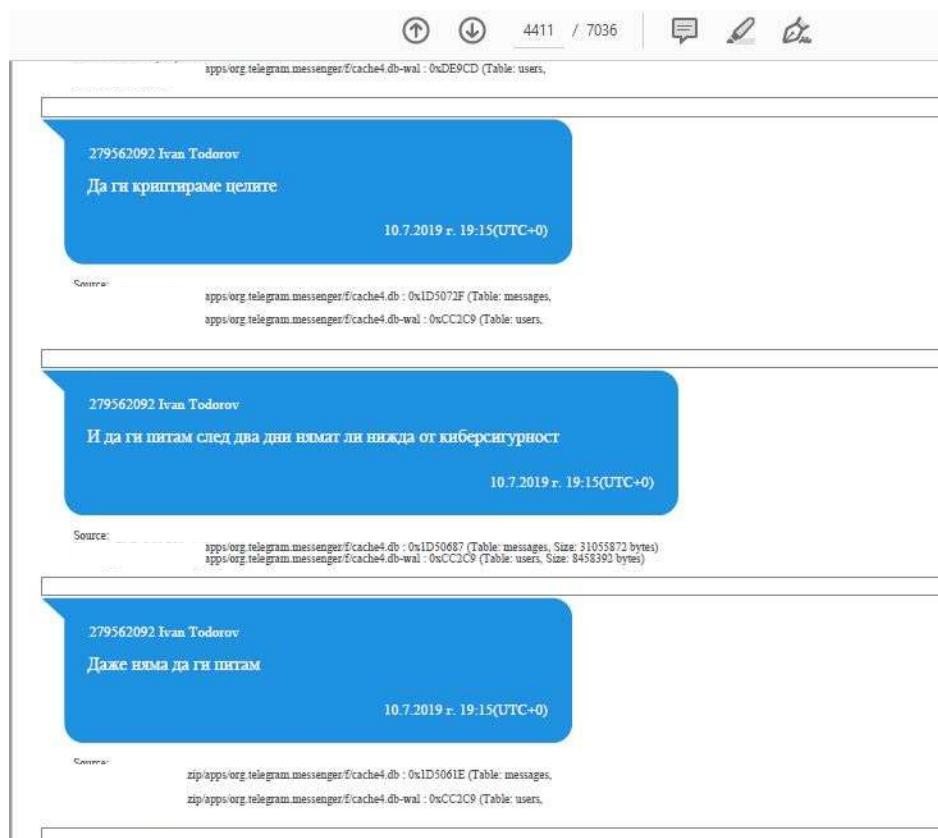
В групата е установена чат комуникация, в която Бойков пише „Хакнахме сървъра... имаме 4-5 инициали но не знам тоя сървър до кви други системи има достъп ще го разгледаме утре след работа то е ся към 7 исках да проверя един вирус.... Дали ще го хване седмицата им“

The screenshot shows a Telegram chat interface with three messages from a contact with ID 571921516. The messages are:

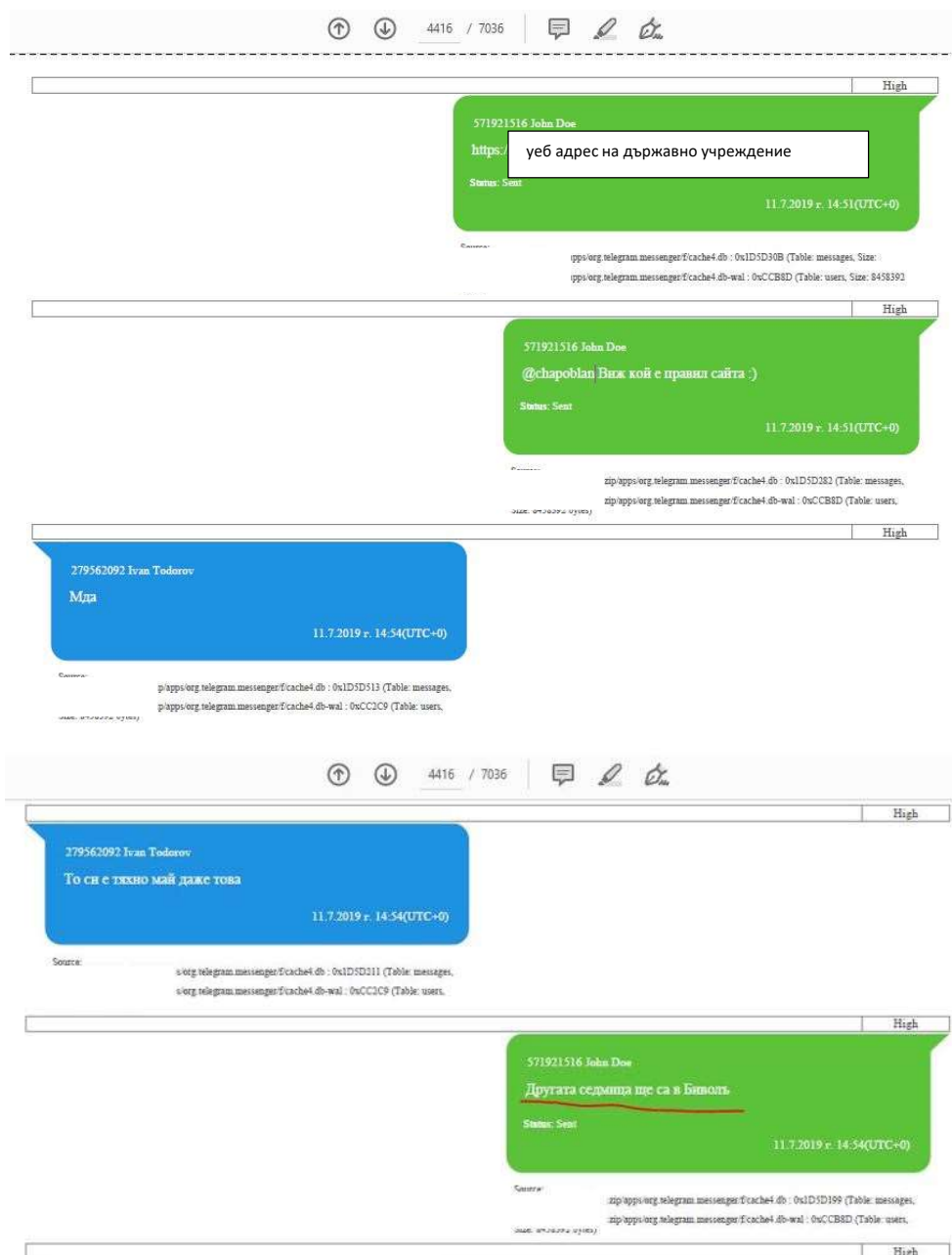
- Message 1: "Хакнахме сървъра... имаме 4-5 инициали", timestamp: 10.7.2019 г. 17:42(UTC+0). Status: Sent. Metadata: /p/apps/org.telegram.messenger/f/cache4.db: 0x1D50B3A (Table: messages, Size: 31055872 bytes); /p/apps/org.telegram.messenger/f/cache4.db-wal: 0xCCB8D (Table: users).
- Message 2: "Но не знам тоя сървър до кви други системи има достъп", timestamp: 10.7.2019 г. 17:42(UTC+0). Status: Sent. Metadata: /zip/apps/org.telegram.messenger/f/cache4.db: 0x1D50A8A (Table: messages, Size: 31055872 bytes); /zip/apps/org.telegram.messenger/f/cache4.db-wal: 0xCCB8D (Table: users).
- Message 3: "Ще го разгледаме утре след работа", timestamp: 10.7.2019 г. 17:42(UTC+0). Status: Sent. Metadata: /apps/org.telegram.messenger/f/cache4.db: 0x1D50A1D (Table: messages, Size: 31055872 bytes); /apps/org.telegram.messenger/f/cache4.db-wal: 0xCCB8D (Table: users).



Няколко часа по-късно Иван Тодоров отговаря „Да ги криптираме целите. И да ги питам след два дни нямат ли нижда от киберсигурност. Даже няма да ги питам“



На следващия ден (11.07.2019 г.), Бойков споделя на Тодоров уеб адрес ***** (на държавно учреждение) и пише „@Charoblan, Виж кой е правил сайта :)“ Тодоров отговаря „Мда. То си е тяхно май даже това.“, на което Бойков пише „Другата седмица са в Биволь“.



В същата група има установена чат комуникация с дата 03.11.2018г., в която Бойков сочи, че има достъп до системата на *застрахователна компания 4*

High

571921516 John Doe
Имам достъп до вътрешната система на **Застрахователно дружество 4**

Status: Sent 3.11.2018 г. 00:58(UTC+0)

Source: ip/apps/org.telegram.messenger/f/cache4.db : 0x645818 (Table: messages, size: 2438392 bytes)
ip/apps/org.telegram.messenger/f/cache4.db-wal : 0xCCB8D (Table: users, size: 8458392 bytes)

High

571921516 John Doe

Status: Sent 3.11.2018 г. 00:58(UTC+0)

Source: ip/apps/org.telegram.messenger/f/cache4.db : 0x6457C7 (Table: messages, size: 2438392 bytes)
ip/apps/org.telegram.messenger/f/cache4.db-wal : 0xCCB8D (Table: users, size: 8458392 bytes)

High

571921516 John Doe
Буквално до портала в който всяка една служителя си качва

Status: Sent 3.11.2018 г. 01:06(UTC+0)

Source: ip/apps/org.telegram.messenger/f/cache4.db : 0x64570C (Table: messages, Size: 31055872 bytes)
ip/apps/org.telegram.messenger/f/cache4.db-wal : 0xCCB8D (Table: users, Size: 8458392 bytes)

като Иван Тодоров пише „Значи да ги гоним за тестове ако не, в новините“

2443 / 7036

ip/apps/org.telegram.messenger/f/cache4.db-wal : 0x0470C (Table: messages, size: 31055872 bytes)
ip/apps/org.telegram.messenger/f/cache4.db-wal : 0xCCB8D (Table: users, size: 8458392 bytes)

High

571921516 John Doe
114k файла и 7GB база в крайна сметка :)

Status: Sent 3.11.2018 г. 04:56(UTC+0)

Source: zip/apps/org.telegram.messenger/f/cache4.db : 0x64568B (Table: messages, size: 31055872 bytes)
zip/apps/org.telegram.messenger/f/cache4.db-wal : 0xCCB8D (Table: users, size: 8458392 bytes)

High

571921516 John Doe
И една безсънна нощ

Status: Sent 3.11.2018 г. 04:57(UTC+0)

Source: zip/apps/org.telegram.messenger/f/cache4.db : 0x64561F (Table: messages, size: 31055872 bytes)
zip/apps/org.telegram.messenger/f/cache4.db-wal : 0xCCB8D (Table: users, size: 8458392 bytes)

2443

High

279562092 Ivan Todorov
Значи да ги гоним за тестове

3.11.2018 г. 07:58(UTC+0)

2444 / 7036

High

279562092 Ivan Todorov
Ако не, в новините
3.11.2018 г. 07:58(UTC+0)

Source: p:\apps\org.telegram.messenger\cache4.db : 0x645483 (Table: messages, Size: 31055872 bytes)
p:\apps\org.telegram.messenger\cache4.db-wal : 0xCC2C9 (Table: users, Size: 8458392 bytes)

High

571921516 John Doe
Трях да мнне известно време
Status: Sent
3.11.2018 г. 11:18(UTC+0)

Source: p:\apps\org.telegram.messenger\cache4.db : 0x64540F (Table: messages, Size: 31055872 bytes)
p:\apps\org.telegram.messenger\cache4.db-wal : 0xCCB8D (Table: users, Size: 8458392 bytes)

High

571921516 John Doe
Не е бях изчакал едната база... 18.7GB е основната база на клиентите
Status: Sent
3.11.2018 г. 11:24(UTC+0)

Source: p:\apps\org.telegram.messenger\cache4.db : 0x645357 (Table: messages, Size: 31055872 bytes)
p:\apps\org.telegram.messenger\cache4.db-wal : 0xCCB8D (Table: users, Size: 8458392 bytes)

Няколко часа по-късно разговорът продължава, като Иван Тодоров пише: „значи може да стане чудесен скандал. Ако съм ще го кача в нета за назидание“

2449 / 7036

High

279562092 Ivan Todorov
ахах
3.11.2018 г. 12:47(UTC+0)

Source: p:\apps\org.telegram.messenger\cache4.db : 0x6482DA (Table: messages, Size: 31055872 bytes)
p:\apps\org.telegram.messenger\cache4.db-wal : 0xCC2C9 (Table: users, Size: 8458392 bytes)

High

279562092 Ivan Todorov
Значи може да стане чуден скандал
3.11.2018 г. 12:47(UTC+0)

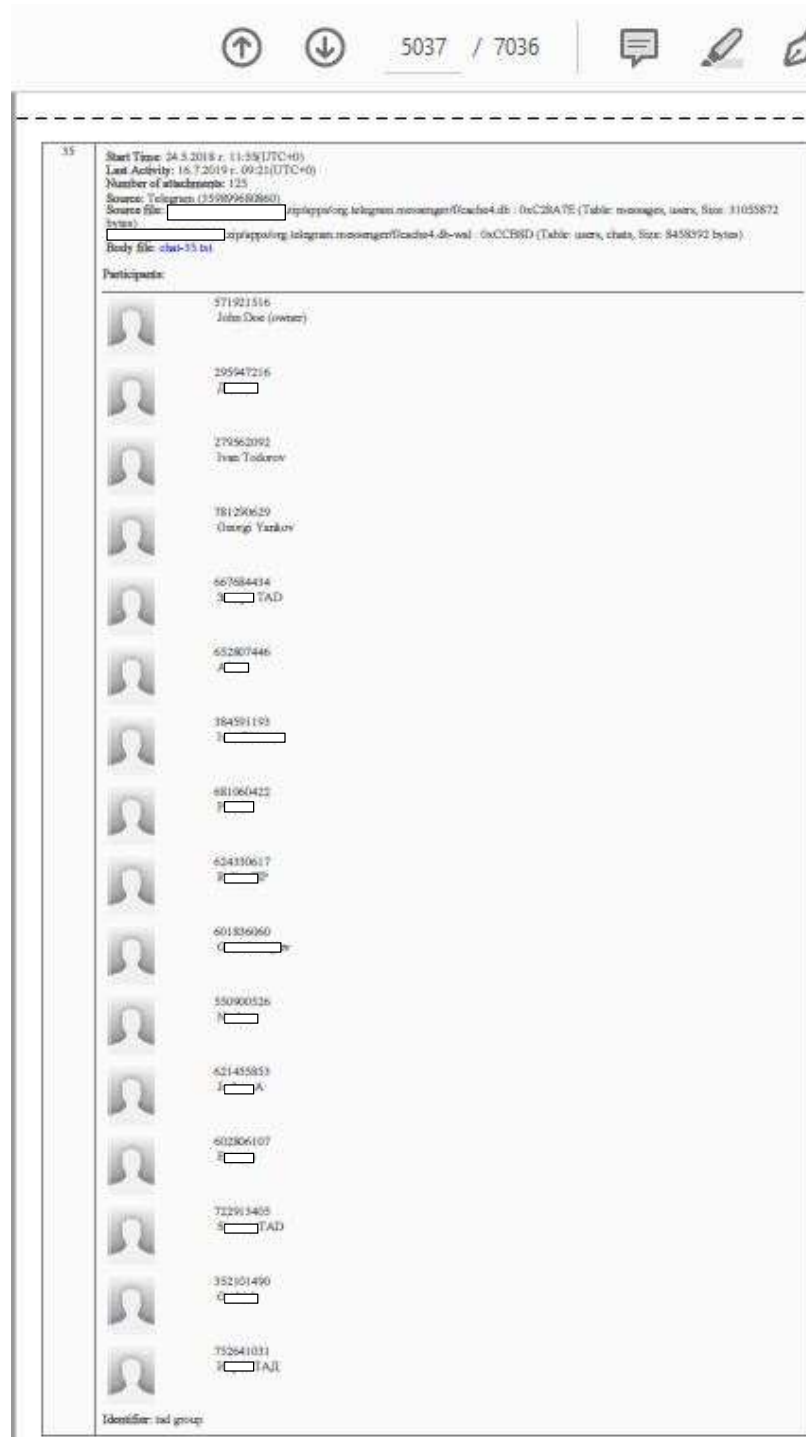
Source: p:\apps\org.telegram.messenger\cache4.db : 0x64825B (Table: messages, Size: 31055872 bytes)
p:\apps\org.telegram.messenger\cache4.db-wal : 0xCC2C9 (Table: users, Size: 8458392 bytes)

High

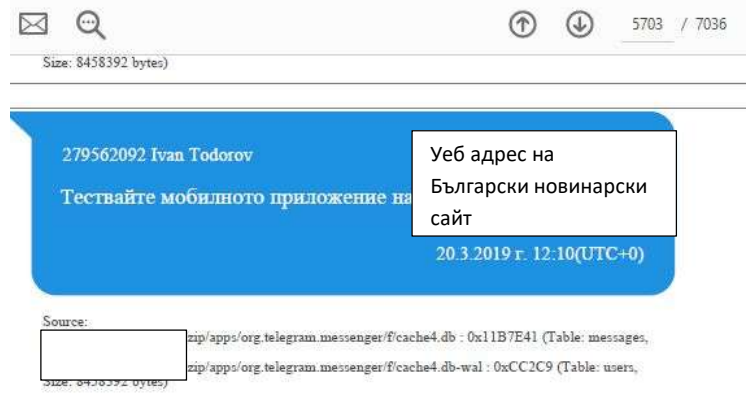
279562092 Ivan Todorov
Ако ако съм ще го кача в нета за назидание
3.11.2018 г. 12:47(UTC+0)

Source: p:\apps\org.telegram.messenger\cache4.db : 0x6481D3 (Table: messages, Size: 31055872 bytes)
p:\apps\org.telegram.messenger\cache4.db-wal : 0xCC2C9 (Table: users, Size: 8458392 bytes)

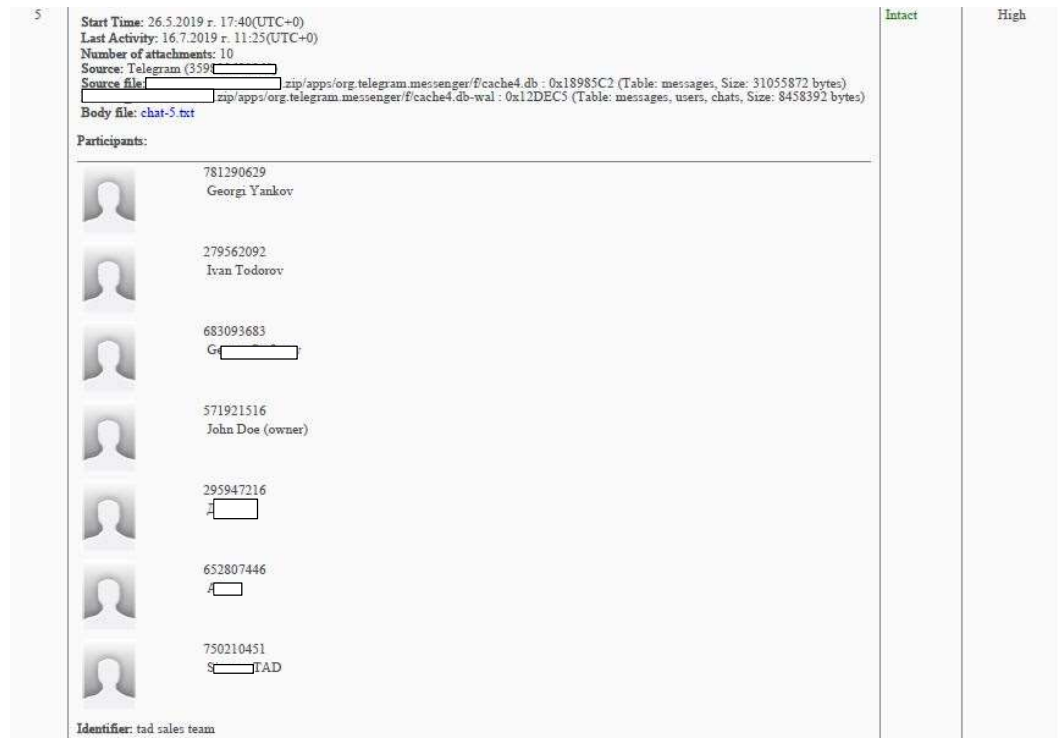
Установен е групов чат с участници с потребителски имена „John Doe“(owner) установен като Кристиан Георгиев Бойков ЕГН *****; „Д “ установен като Д.Х. ЕГН *****; „Ivan Todorov” установен като Иван Тодоров ЕГН *****; „Georgi Yankov“ установен като Георги Янков ЕГН *****; „З ТAD“ установен като З.М. ЕГН *****; „А “ установен като А.П. ЕГН *****; I v“ установен като И.П. ЕГН *****; „P “, „R P“, „G v“ установен като Г.Г. ЕГН *****; „N “ С.Н. ЕГН *****; „J A“, „E “, „S TAD“, „G “ установен като Г.А. ЕГН *****; „И ТAD“ установен като И.А. ЕГН *****;



На 23.03.2019г. Иван Тодоров пише: „Тествайте мобилното приложение на уеб адрес на Български новинарски сайт“



Следващият групов чат с участници с потребителски имена „Georgi Yankov“ установен като Георги Янков ЕГН *****; „Ivan Todorov“ установен като Иван Тодоров ЕГН *****; „G v“, „John Doe“(owner) установен като Кристиян Бойков ЕГН *****; „Д “ установен като Д.Х. ЕГН *****; „А “ установен като А.П. ЕГН *****; „S TAD“.



В чата е установена публикация от Иван Тодоров: „https://www.“ (български уеб сайт за публикуване на обяви) Тук може да се ориентираме също за големи компании, като скипваме някои които е ясно, че ще ни рязнат. Ако не, ще получат CV с троянски катър.“



[Redacted]

279562092 Ivan Todorov
<https://www.български.уеб.сайт.за.публикуване.на.обяви>
6.6.2019 г. 06:50(UTC+0)

Source: [Redacted]
zip/apps/org.telegram.messenger/cache4.db : 0x19BC392 (Table: messages,
zip/apps/org.telegram.messenger/cache4.db-wal : 0xCC3C9 (Table: users,

279562092 Ivan Todorov
Тук може да се ориентираме също за големи компании, като скипваме някои които е ясно, че ще ни резнат.
6.6.2019 г. 06:51(UTC+0)

Source: [Redacted]
zip/apps/org.telegram.messenger/cache4.db : 0x19BC543 (Table: messages, Size: 31055872 bytes)
zip/apps/org.telegram.messenger/cache4.db-wal : 0xCC3C9 (Table: users, Size: 8458392 bytes)

279562092 Ivan Todorov
Ако не, ще получат CV с троянски катър
6.6.2019 г. 06:51(UTC+0)

Source: [Redacted]
zip/apps/org.telegram.messenger/cache4.db : 0x19BC4C2 (Table: messages,
zip/apps/org.telegram.messenger/cache4.db-wal : 0xCC3C9 (Table: users,
size: 8458392 bytes)