И. А. :

Тази кореспонденция я водихме посредством приложението „Телеграм“. По време на разговора Кристиян Бойков ме попита дали ще му помогна да „хакнем“ Национална агенция по приходите, като уточни, че иска да „хакнем“ домейните nap.bg и nra.bg, както и всички поддомейни на НАП. Кристиян искаше да направим пробив в информационната система на НАП и да свалим база данни. Аз се съгласих, но му казах, че ще го направим по-късно, тъй като отивам на зъболекар. С това разговорът ни за НАП приключи. Аз се съгласих само, защото не ми се занимаваше с него, но нямах намерението да го правя и аз лично не съм правил нищо.

По късно, мисля, че след около три седмици видях в един общ чат на компютърна тематика, с над 50 участника отново в „Телеграм“, че Кристиян се интересува от айпи адресите на nap.bg и nra.bg. Малко след това някой от групата, не си спомням кой точно, пусна айпи адресите на nap.bg и nra.bg. Тогава Кристиян написа:“ей, сега ще видите какво ще стане, момчета“.

Поради това, което разказах когато изтече базата данни на НАП веднага си помислих, че Кристиян Бойков го е направил. Помислих си, че той е записал базата данни на НАП и я изпратил на медиите...

...Искам да поясня, че Кристиян ни задължаваше мен и З да правим снимки на откритите уязвимости на сайтовете и да ги пазим. Това се правеше от една страна, за да се докаже на клиента, че действително има уязвимост, а от друга страна Кристиян впоследствие експлоатираше тази уязвимост, като записваше различни бази данни на външен хард диск. Кристиян колекционираше бази данни от различни сайтове, като ги записваше на диска с имената на сайтовете. Кристиян записваше базите данните на клиентите, с които имахме сключен договор, но без тяхно съгласие. Лично от него знам, че е правил тестове за уязвимости на сайтове, без знанието и съгласието на собствениците им и също е записвал базите им данни на външния хард диск. Кристиян се хвалеше, че продава различните бази данни в един хакерски форум Raid Forums. Кристиян Бойков ми е предоставял да разглеждам лично този диск. Когато ми го даде да го разгледам в него имаше над 500 GB информация. Спомням си, че в него бяха записани базите данни на следните сайтове: mon.bg, ….....bg, ...bg, ddos.....bg. Впоследствие мисля, че беше добавил и базата данни на .....bg. Информацията свалена от различните сайтове и съхранявана от Кристиян на горепосочения диск съдържаше основно потребителски имена и пароли на администраторите на сайта. Спомням си, че имаше имена, презимена, дата на раждания, ЕГН-та, имейли, айпи адреси...

...Не си спомня точно кога, но Кристиян ми се похвали, че е свалил голяма база данни, съдържаща регистрационните номера на много автомобили, както и лични данни на техните собственици – имена, ЕГН-та, имейли. Кристиян ми каза, че държи тази база данни на много сигурно

място и има информация за всички автомобили в България и техните собственици.

Искам да уточня, че за въпросния хард диск и съдържащата се в него информация знаеха всички служители на фирмата, които работеха там към датата на моето постъпване. Този хард диск непрекъснато стоеше у Кристиян Бойков. Носеше в раницата си като идваше на работа, виждал съм го да го вади оттам като идва и да го прибира в раницата преди да си тръгне. Давал го е на З. М. да го разгледа пред мен, на мен също го е давал да го разгледам. Тогава ни го даде за две минути, за да видим какви сайтове е свалял вътре и докато го разглеждахме, през цялото време Кристиян беше при нас.

Кристиян ме караше да допълвам данните в хард диска с други данни, които съм достъпил нерегламентирано от различни сайтове, които не са на наши клиенти. Аз не се съгласих да правя това, защото знам, че не е законно. Единствено открих уязвимост в сайта на А., за които Кристиян ме увери, че предстои да станат наш клиент. Той буквално ми каза, че бил говорил със собственика на „А“. Това стана през април 2019 г., не помня точната дата. Тогава намерих я без да ползвам готови програми, а с ръчно претърсване. След това пратих линк към уязвимостта на Кристиян, изпратих му го в личен чат. После не знам той какво е направил с уязвимостта. Веднага след това Кристиян се обади по телефона на някого и му каза, че съм успял да хакна сайта на А.. Същият следобяд, когато Иван Тодоров дойде в офиса ни, Кристиян му съобщи и на него, че съм хакнал сайта на А.. Тогава се усъмних, че Кристиян ме е излъгал, че А. ще станат наш клиент. По-късно проверих в системата на фирмата ни и видях, че наистина няма сключен договор с тях. След това станах по-предпазлив към информация, дадена от Кристиян относно това кои сайтове са наши клиенти.

Искам да уточня, че Кристиян и Иван от една страна, както и Кристиян и Георги, от друга страна имаха сякаш по-тайни отношения, защото се отделяха да си говорят настрани от нас, останалите – излизаха на терасата да пушат и да си говорят тайно. Иван и Георги не съм ги виждал да се отделят и да си говорят тайно помежду си. Иван Тодоров и Георги Янков знаеха за диска на Кристиян с хакнатите данни – виждал съм Кристиян да го ползва пред тях, както и пред останалите служители в офиса. Предполагам, че Иван е поставил на Кристиян задачата да хаква различни сайтове и после да им предлага да станат наши клиенти. Смятам така, защо Кристиян е просто служител и не би направил нещо такова на своя глава, докато работи във фирмата. Лично аз съм го виждал по време на работа да тества сайтове както на наши клиенти, така и на такива, които не са ни клиенти.

В началото на м.април 2019 г., малко след случката със сайта на ……., Кристиян влезе в офиса ни, като се заливаше от смях. Когато го попитахме какво се е случило, той ни каза, че е продал някаква база данни за 15 000, не си спомням в каква валута е тази сума. Доколкото разбрах, купувачът е бизнесмен – българин, доколкото помня спомена, че е

от конкурентна фирма, но не е споменавал други подробности. Каза също, че купувачът му е дал половината от тази сума на ръка, в брой, а остатъкът ще му плати по-късно по друг начин.

Мен Кристиян ме е обучавал как да хаквам сайтове. Казвал ми е, че е добре, ако искам да хакна някой сайт, да не работя през моя доставчик на интернет, а да кракна уай-файът на съседите, за да не хванат. Той ми се похвали, че самият той винаги работи така. Сещам се също, че веднъж Кристиян на всеослушание каза на мен и другите колеги в офиса, че е добре, ако правим нещо незаконно, напр. ако сканираме за уязвимости сайто ве, които не са наши клиенти, да използваме VPN „TOR Phantom“, т.к. си сменя непрекъснато IP адреса, през 10-15 мин и така не може да се засече.

Искам да добавя също, че след случката с ……., Кристиян ми каза, че още два сайта ……..bg и ……..bg ще ни станат клиенти и ми каза да ги тествам за уязвимости. За името на втория сайт не съм много сигурен.

Спомена, че са му предложили 2 000 лв., ако намери уязвимости в единия от сайтовете и именно това ме усъмни, че отново се опитва да ме накара да осъществя за нерегламентиран достъп до тези сайтове. Не каза кой му предлага тази сума.

Относно случая, при който Кристиян беше хакнал базата данни на ……. мога да кажа, че във въпросния хард диск, за който разказах, имаше папка озаглавена ……...bg и ……...bg, но те бяха празни към момента, към който Кристиян ми ги показа – към средата на м.април 2019 г. Тогава Кристиян ми предложи, ако искам да си сваля данни от хард-диска му.

Този диск Кристиян ми го е показвал веднъж и го уе използвал 2-3 пъти в офиса, за да търси други данни – търсеше хора по име, по ЕГН, по IP, но не знам какви хора и защо е търсил.

И.П.

Кристиян Бойков бе назначен на работа малко след мен, имам предвид в края на 2017г. Направи ми впечатление, че е с голямо самочувствие и изключително надменен. Той бе назначен след като стана известен с хакването на ……. За това време Кристиян се сближи доста със собственика на фирмата Иван Тодоров. Постепенно започнаха да идват клиенти, които желаеха да се правят тестове, относно киберсигурност на техните платформи и сайтове. Но все пак броя на клиентите е недостатъчен, затова не съм сигурен кой го предложи Иван или Кристиян, част от политиката на фирмата за набиране на клиенти да бъде тестването на сайтове на различни дружества без тяхно знание и в последствие да ги набират като клиенти. Тази политика на фирмата се

коментираше постоянно в офиса основно между Иван и Кристиян, като двамата си говореха, че трябва да се изготви списък с най-големите български сайтове, които да бъдат тествани без знанието на техните собственици, като след това бъдат привлечени като клиенти.

Впоследствие разбрах, че Кристиян е направил такъв тест на сайта на …… със знанието на Иван Тодоров, от който бе намерена уязвимост xss (cross – site scripting), която би могла да осигури достъп до сесии на потребители и да извърши пренасочването им към други страници, както и иницииране на заявки от потребителите без тяхното знание. Мисля, че беше малко след като Кристиян постъпи на работа. За този тест разбрах след като Иван Тодоров ми каза да отговоря на гневен имейл, изпратен от Н.л. Аз му отказах, тъй като първото писмо до Н. л. бе изпратено от Кристиян и чисто технически не беше коректно, още повече че беше проведен тест без тяхно съгласие, което в крайна сметка не е правилно. Аз не съм се съгласявал да се провеждат подобни тестове. Поради тази причина казах на Иван, че най-добре би било да се извинят на Н. л. Кристиян постоянно критикуваше държавата и ниското ниво на киберсигурност на различните държавни платформи и сайтове. Дори няколко пъти с насмешка казваше, че има предчувствие за дадена платформа какви уязвимости има без да конкретизира, а Иван Тодоров, отново на майтап му казваше „ми дай да видим какво имат“. Тези разговори между двамата аз винаги съм възприемал на шега, но винаги съм подозирал, че Кристиян прави нерегламентирани тестове на различни платформи, защото SQLMap програмата, с която правеше тестовете понякога бе включена и без да имаме клиенти. Спомням си че пред мен се е хвалил, че е имал достъп до системата, която управлява водни струи за поливане пред парламента и ни казваше дали искаме да пусне отделни струи и да ходим да видим на място, дали действат. Също така се хвалеше, че е компрометирал «хаквал» безжичния интернет на съседите си. В последните дни на моята работа в «Тад Груп» ЕООД Кристиян се похвали, че е има осигурен администраторски достъп до сайта на ……...

Спомням си че Кристиян ме помоли веднъж лично и извънслужебно да му помогна за съдействие, а именно да компрометира, т.е да осъществи достъп до сайт на фирма, която се занимава с туристически услуги, без знанието на собствениците й. Доколкото си спомням това се случи в началото на 2019г., но не мога да конкретизирам датата. Не си спомням името на дружеството. Не зная дали впоследствие Кристиян е успял да осъществи достъп до тази база данни. Тогава предположих, че целта на Кристиян е извличане на списъка на клиенти, тъй като неговото семейство има подобна фирма и най-вероятно е целял набиране на нови клиенти, посредством осъществяване на достъп до базата данни на фирмата.

Искам да поясня, че докато работех в ТАД ГРУП ЕООД Кристиян Бойков изготви списък с най-големите български сайтове по потребителски посещения в интернет, до които да се осъществи достъп без знанието и

съгласието на собствениците му. Аз лично не съм виждал този списък, само съм чувал за него да говорят Кристиян и Иван. Доколкото аз зная по този начин е тествана само Н. л., нямам представа дали са тествали и други сайтове впоследствие. Вече не си спомням за кои други сайтове се коментираше, че са включени в този списък.

Л.Н.

Не си спомням точната дата, но мисля, че беше в края на 2016г. или началото на 2017г., категорично не си спомням кога беше, не си спомням и дали бях започнал работа или ходех все още на обучения в ТАД ГРУП когато разбрах от моите колеги, че са установили уязвимост, чрез която се разкриват потребителското име и парола на потребители, ползващи услугите на ....bg, собственост на „Н.“. Доколкото зная тогава не е сваляна база данни от ....bg, а тестовете са правени с личните пощи на колегите ми. Иван Тодоров също беше наясно, тъй като това се обсъждаше в офиса. Още повече, че не се правеха никакви тестове без Иван Тодоров да ги одобри. Тогава не разбрах кой от тримата провеждаше тези тестове и установи уязвимост в ....bg, но и тримата знаеха, че се провежда такъв тест. Тогава не си спомня кой направи контакт с Н., собствениците на ....bg и ги уведоми за тази уязвимост. Аз разбрах от колегите, че са установили контакт с Н. и са им предложили да направят официален тест на цялата платформа, но те отказали. При този отказ Иван Тодоров каза на всички в служители в офиса, че има право след 14 дневен срок да оповести откритото в публичното пространство за откритата уязвимост в сайта на ....bg. Обясни, че такива са правилата по закон и че трябва се изчакат 14 дин, за да може „Н.“ да си коригират системите. След този срок фирмата обяви, че ....bg имат уязвимости публично чрез сайта на „ТАД ГРУП“, а оттам и чрез други сайтове. Не зная кой бе правил теста на ....bg, нито кой бе оповестил новината публично, но всичко това бе със знанието на собственика Иван Тодоров. Зная също така, че Н. са заплашвали Тад Груп, че ще ги съдят, вероятно защото са осъществили достъп до сайта им и са го оповестили без тяхно съгласие...